



Windar renovables

Normativa de seguridad de la información

Índice

1. Objetivo
2. Uso de información
3. Uso de sistemas de Información y recursos TIC
4. Usos prohibidos, ilegales o no aceptables
5. Supervisión y verificación del uso aceptable
6. Intercambio de Información
7. Política de Control de Accesos
8. Política de uso de correo electrónico
9. Política de uso de Soportes Externos
10. Uso responsable de internet. Restricciones a la navegación.
11. Uso de las licencias de software
12. Tratamiento de datos de carácter personal
13. Gestión de incidencias
14. Uso de teléfonos móviles corporativos
15. Organización de la Seguridad de la Información
16. Programas y dispositivos de control y monitorización
17. Uso de la inteligencia artificial
18. Responsabilidades derivadas del incumplimiento de la política

1. Objetivo

El presente documento tiene por objeto establecer las normas y principios que se deben de considerar por parte de los usuarios de WINDAR durante la utilización de los medios y recursos tecnológicos y, en general los sistemas de información facilitados por la organización para el desarrollo de las actividades, a fin de asegurar una protección adecuada de la información de la organización.

La información, propia o de nuestros clientes, es un recurso fundamental para la organización y requiere de una protección adecuada a fin de asegurar un desarrollo efectivo de las operaciones de la organización, y el cumplimiento de los requisitos contractuales y legales existentes al respecto, incluyendo los derivados de la normativa de protección de datos personales.

La presente normativa de seguridad de la información, se ha realizado en base a los principios y compromisos asumidos por la dirección de WINDAR a través de la [Política de Seguridad de la información](#) que se encuentra aprobada y publicada a través de la página web de la organización.

Esta normativa de seguridad se ha desarrollado teniendo en consideración los principales estándares y normas de referencia (en particular, la norma ISO 27001 de seguridad de la información), así como las necesidades derivadas de los requisitos contractuales y legales de aplicación a la organización (en particular, aquellos derivados de la normativa de protección de datos personales).

Este documento será de aplicación a todos los usuarios que tengan acceso a la utilización de los sistemas de información propiedad de la empresa, incluyendo entre estos los equipos informáticos (PC, portátiles, servidores), infraestructuras de comunicaciones, conexión a redes internas o externas, terminales, software, hardware, servicios telemáticos, infraestructura de redes, accesos a Internet, soportes no automatizados (papel), y, en general, todos los recursos a los que tenga acceso el personal o usuario para el cumplimiento de tareas asignadas en el ámbito laboral.

2. Uso de información

La información es un activo de trascendental importancia para la organización y que requiere, por lo tanto, de una protección adecuada que reduzca los riesgos asociados a pérdidas de confidencialidad, integridad o disponibilidad de la misma. Para asegurar esta protección, desde WINDAR se ha desarrollado la presente normativa de seguridad de aplicación por parte de todos los usuarios de la organización con acceso a la información y a los sistemas de tratamiento.

Con carácter general, los usuarios deberán de considerar las siguientes normas y directrices:

- El acceso y uso de información por parte de los usuarios se limitará a lo estrictamente necesario para un eficaz desempeño de su actividad profesional, no pudiendo accederse o usarse información para la cual no disponga de autorización, o que no sea necesaria para el desarrollo de sus tareas salvo que autorización expresa de los responsables designados a tal efecto. En general se aplicarán en la organización los principios de “mínimo privilegio” y “necesidad de conocer”.
- El acceso a la información de la organización, se controlará mediante las normas definidas en el apartado correspondiente del presente informe.
- En WINDAR se dispone de diferentes tipos de información de mayor o menor relevancia o criticidad, que requerirá la aplicación de medidas adicionales. En este sentido, se considera la existencia de información de carácter pública o sin restricciones, así como de información confidencial o sujeta a restricciones o limitaciones de acceso, atendiendo a la importancia de la confidencialidad de la misma. Desde WINDAR se habilitarán los mecanismos de clasificación y etiquetado de la información a fin de permitir al usuario conocer el tipo de información a la que esté accediendo y las medidas de seguridad adicionales que debe considerar en consecuencia.
- Con carácter general, la información de WINDAR deberá de ser tratada por el personal siguiendo las directrices marcadas a través de esta normativa, y aplicando, en general, la necesaria protección y cuidado sobre la misma, atendiendo a las necesidades de confidencialidad, integridad y disponibilidad de la información y los servicios.
- El acceso y uso de la información a través de los sistemas facilitados por la organización, se ajustará a lo definido a través de la presente normativa, en los apartados que se desarrollan a continuación.
- El intercambio y almacenamiento de la información de WINDAR deberá de ajustarse igualmente a las sistemáticas y medios de almacenamiento e intercambio que se detallan en la presente normativa de seguridad.

3. Uso de sistemas de Información y recursos TIC

Para un adecuado desarrollo de las actividades de los usuarios, WINDAR pondrá a su disposición los medios y sistemas de tratamiento necesarios, y habilitará los mecanismos de accesos pertinentes para acceder y tratar la información que precise para el desarrollo de sus funciones. Con carácter general, el uso de los sistemas informáticos que se pongan a su disposición deberá de quedar sujeto a las siguientes normas de uso:

- Los sistemas de información y recursos TIC que se le faciliten a los usuarios, pertenecen a la empresa y el uso de los mismos debe emplearse exclusivamente con propósitos laborales, salvo autorización expresa por parte de la dirección o los responsables designados a tal efecto.
- Es responsabilidad del usuario, en la medida de sus posibilidades y con la colaboración de los responsables y el área de TI el cuidado y buen trato de los recursos informáticos asignados, siguiendo las normas y buenas prácticas definidas a través de la presente normativa así como de otras normas, políticas o buenas prácticas que le sean comunicados formalmente.
- Los equipos disponen de una configuración de seguridad por defecto definida por los responsables designados de WINDAR que da respuesta a las necesidades de la organización para hacer frente a las amenazas que le puedan afectar (esto incluye sistemas antivirus, limitaciones de acceso, actualizaciones de seguridad, herramientas de monitorización,...).
- Asimismo, los equipos informáticos se entregan a los usuarios con las aplicaciones, software y utilidades que necesitan para el desarrollo de sus funciones, tratando de limitarse aplicaciones o funcionalidades no necesarias que puedan incrementar los riesgos sobre los sistemas.
- Queda expresamente prohibido la modificación de esta configuración de seguridad inicial de los equipos, así como la instalación de software adicional sin la previa autorización por parte de los responsables correspondientes, la cual se deberá de realizar a través de la herramienta de ticketing disponible a tal efecto.
- Del mismo modo, la instalación de cualquier software adicional que sea requerido por el usuario, deberá de quedar sujeta a la previa autorización y validación por parte de los responsables correspondientes y de los administradores de sistemas, la cual se gestionará a través de la herramienta de ticketing habilitada a tal efecto.
- Con carácter general, y salvo excepciones debidamente justificadas, WINDAR habilitará los mecanismos necesarios de control de accesos y asignación de privilegios adecuados para limitar los permisos de los usuarios para modificar la configuración de los sistemas, requiriéndose para ello la correspondiente autorización y la participación de los administradores de sistemas.

- Toda la información de WINDAR deberá de almacenarse y accederse de manera centralizada a través de la estructura de carpetas que se habilite o de las herramientas de gestión disponibles en la organización a tal efecto (CEDOC), lo cual permite, entre otros aspectos, una adecuada disponibilidad y accesibilidad de la misma, y la aplicación de medidas de seguridad de manera consistente y centralizada.
- Salvo autorización expresa, se prohíbe el almacenamiento de información a nivel local en los equipos, o en otros soportes o medios de almacenamiento (dispositivos USB, soportes externos, utilidades de almacenamiento en la nube tipo Dropbox, Drive,...) .
- Los recursos informáticos (puestos de usuarios, servidores portátiles, soportes de almacenamiento...) deberán de ser ubicados y orientados de modo que se minimice la posibilidad de accesos físicos o visuales no autorizados. WINDAR habilitará los mecanismos necesarios para asegurar esta correcta ubicación, debiendo los usuarios de notificar a los responsables correspondientes en caso de que detecte alguna desviación respecto a esta medida, para que se puedan tomar las medidas correctoras necesarias.
- Igualmente, los equipos informáticos deberán de ubicarse de modo que se minimicen los riesgos derivados de amenazas de índole físico (como pueden ser humedad, suciedad, polvo, golpes o caídas,...) o el impacto que estas amenazas pueden provocar sobre la información o los servicios de WINDAR. Desde WINDAR se tendrá en consideración este aspecto en el momento de instalación de los equipos, si bien los usuarios deberán colaborar, en la medida de sus posibilidades, en la aplicación de esta medida, debiendo de notificar a los responsables correspondientes en caso de que detecte alguna desviación al respecto.
- WINDAR desarrollará los procesos de mantenimiento preventivo o correctivo necesarios para asegurar que los equipos informáticos se encuentran en las condiciones físicas adecuadas para asegurar su correcto funcionamiento, así como para asegurar que los mismos mantienen la configuración de seguridad necesaria.
- Para ello, WINDAR se reserva el derecho de acceder a los equipos de los usuarios en cualquier momento, por parte de los administradores de sistemas y los responsables designados a tal efecto, a fin de asegurar un adecuado mantenimiento de los equipos, según las condiciones definidas en el apartado correspondiente de la presente normativa.
- Con carácter general el usuario tomará todas las precauciones y medidas de seguridad oportunas para salvaguardar el material, contenido e información que le han sido confiados, incluyendo ordenadores, soportes magnéticos u ópticos o cualquier dispositivo que contenga información de WINDAR.
- Los usuarios a quien les hayan sido designados estos dispositivos deberán de, en la medida de sus responsabilidades, custodiar adecuadamente estos equipos, y adoptar medidas orientadas a evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- En este sentido, se deberán de tener en cuenta acciones como no dejar los equipos desatendidos cuando esté en instalaciones de cliente, o, en general, fuera de las instalaciones de la organización, especialmente en zonas donde puedan ser accedidos por usuarios no autorizados.
- Del mismo modo, se deben adoptar acciones como no dejar los equipos o dispositivos móviles a la vista cuando estos se trasladen fuera de las oficinas o se lleven en vehículos, debiendo aplicar medidas y buenas prácticas orientadas a minimizar su exposición, como puede ser, por ejemplo, no mantener estos dispositivos en los vehículos de los usuarios de forma innecesaria o indefinida (por ejemplo, en traslados o movimientos fuera del ámbito laboral).
- En los casos en los que se deba dejar desatendido, los usuarios deberán de asegurarse de dejar el equipo bloqueado o apagado.
- En caso de robo o pérdida del equipo o dispositivos, los usuarios deberán de notificar dicha situación, con la máxima celeridad posible al servicio de soporte a través de las utilidades habilitadas a tal efecto. En la comunicación de la incidencia, el usuario deberá de facilitar los detalles del incidente que le sean posibles y deberá de indicar la información que pueda verse afectada (ya sea porque se encuentra almacenada en los propios equipos, o porque se pueda acceder a ella a través de las utilidades y aplicaciones instaladas en el mismo)
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, modificación de permisos, etc.) que originaron la entrega de un recurso informático móvil, el dispositivo deberá de ser devuelto según el procedimiento de baja definido en la organización, debiendo este de ser devuelto al área IT, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

4. Usos prohibidos, ilegales o no aceptables

Las acciones descritas a continuación están estrictamente prohibidas, o no se considerarán aceptables por la Dirección de WINDAR, por poder suponer actos ilegales o que pongan en grave riesgo la información o los activos de la organización:

- Divulgar información considerada como confidencial, secreta o de uso restringido a personas ajenas a la organización, o a personas no autorizadas, que pueda provocar daños o perjuicios a la empresa. Los empleados deberán de mantener la más absoluta confidencialidad sobre la información a la cual puedan tener acceso, especialmente la información de nuestros clientes, o aquella que contenga datos de carácter personal, para lo cual se comprometen a cumplir el Acuerdo de Confidencialidad que se incluye en el presente documento.
- Con carácter general, los usuarios no podrán acceder o hacer uso de información sobre la cual no se le haya concedido autorización o sea estrictamente necesaria para el desarrollo de las actividades laborales que tenga encomendadas. En caso de que los usuarios detecten un posible o potencial acceso a información para la cual no tenga autorización, este deberá de comunicarlo como incidencia a través de la herramienta de ticketing habilitada a tal efecto.
- El acceso a Internet se limitará a aquellos servicios o utilidades estrictamente necesarias para el desarrollo de nuestras actividades, no permitiéndose accesos con fines recreativos, personales o ajenos (o incompatibles) a nuestras actividades, salvo autorización expresa de los Responsables designados.
- Está prohibido manipular líquidos, comidas, bebidas cerca de los equipos informáticos, o realizar otras acciones que puedan originar directa o indirectamente su mal funcionamiento, siendo el usuario responsable por el deterioro del mismo.
- Alterar de forma total o parcial los componentes hardware, software y las configuraciones de los sistemas operativos de los equipos informáticos asignados al mismo usuario o a otros usuarios, sin la debida autorización
- Intentar acceder a recursos sin autorización, mediante la utilización de herramientas intrusivas, descifre o uso no autorizado de contraseñas, explotación de vulnerabilidades o cualquier otro medio no permitido.
- No guardar con la debida diligencia las claves, contraseñas, nombres de usuario o cualesquiera otros identificadores que pudieran facilitarse al trabajador para utilizar cualquiera de las herramientas, o para acceder a los equipos o sistemas de la Empresa.

- Cargar o introducir de manera deliberada archivos que contengan virus, troyanos, gusanos, archivos dañados, o software similar que pueda perjudicar el funcionamiento de los equipos de la red. Los usuarios deben considerar las pautas o buenas prácticas que se le trasladen desde la Organización para tratar de minimizar este tipo de riesgos.
- Usar los servicios de la red de manera que se pueda dañar, deshabilitar, sobrecargar o deteriorar algún otro equipo o sistema de la organización.
- Conectar a la red de la organización equipos no autorizados, salvo en las excepciones y en los recursos habilitados por WINDAR a tal efecto (por ejemplo, uso de la WIFI de invitados)
- Enviar correo spam, indiscriminado, o encadenado, o no autorizado o consentido previamente por los destinatarios.
- Realizar ataques de denegación de servicio que causen daño o inutilización de los activos de información de la organización.
- Suplantar la identidad de otro usuario o entidad o engañar o confundir sobre el origen de las comunicaciones u otro contenido con fines fraudulentos, inapropiados, o que no sean estrictamente necesarios para el correcto desarrollo de las actividades de WINDAR.
- El acceso a registros, logs, información de tráfico o accesos, o la monitorización de cualquier red o sistema, sin que estas actividades se realicen con fines necesarios para los desarrollos realizados, o se ajusten a las necesidades del proyecto.
- Cualquier actividad que intente la recopilación de información de cualquier equipo o sistema con propósitos no establecidos ni acordados previamente.
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo sin la previa autorización para ello, o sin que sea necesario para el desarrollo de las actividades de la organización.

5. Supervisión y verificación del uso aceptable

El uso inapropiado, abusivo, o que escape a los hábitos tolerados de los servicios de comunicación y de los medios tecnológicos será sancionado con la eliminación del acceso a los recursos, la aplicación de las sanciones disciplinarias derivadas por incumplimiento de los términos y condiciones que emanen de la relación laboral, además de las sanciones legales establecidas en la normativa vigente aplicable.

La empresa podrá realizar las investigaciones y controles que resulten necesarios tanto de los equipos PCs y portátiles, como de las herramientas facilitadas al usuario por parte de la empresa, lo que incluye entre otros el correo electrónico corporativo, dispositivos de tipo Tablet, Smartphone o similar, etc. dentro del ámbito de potestades de control del empresario del Artículo 20.3 del Estatuto de los Trabajadores.

El control y acceso a los medios facilitados por la empresa, incluyendo los documentos generados por los mismos y las comunicaciones que partan de los mismos podrá ser llevado a cabo sin una justificación específica, de forma temporal o permanente, dada cuenta la naturaleza de dichos medios como herramientas de producción facilitadas por la empresa.

El control de estos medios se llevará a cabo sin dañar y sin atentar contra la dignidad o intimidad del usuario, dada cuenta del conocimiento que tiene éste del objeto y la existencia del presente control y fiscalización a la que los usuarios son sometidos. Las finalidades genéricas de este control son las siguientes:

- Protección de los sistemas y la red informática y de los equipos que lo conforman, a fin de proteger la integridad del Sistema y la Seguridad de la Información.

- Garantizar la continuidad del trabajo en el caso de que el usuario se ausente por razón de enfermedad, vacaciones u otras similares.
- Prevención de la responsabilidad frente a terceros.
- Comprobación de cumplimiento de las obligaciones laborales del usuario.
- Comprobación de la existencia o no de un uso abusivo o indebido de los medios tecnológicos facilitados por la empresa, ya sea para usos personales, usos indebidos o en general usos para los que el usuario no haya sido debidamente autorizado.

Por tanto, todos los contenidos, informaciones, ficheros almacenados en el mismo, incluida la información temporal, podrán ser accedidos por parte de la empresa o de los responsables designados al efecto.

El alcance de estos procedimientos de control o inspección se notificarán a todos los usuarios de tal forma que quede constancia pública de los mismos.

El presente documento plantea una serie de recomendaciones que regulan el adecuado uso y disponibilidad de los recursos informáticos, comprometiéndose la empresa a su difusión hacia todo el personal laboral. Los usuarios que, de forma reiterada, deliberada o por negligencia los infrinjan, quedarán sujetos a las actuaciones técnicas o disciplinarias que se estimen oportunas.

6. Intercambio de Información

Para un adecuado desarrollo de las actividades laborales, podrá ser necesario por parte de los usuarios el intercambio de información tanto con usuarios o colaboradores internos, como con usuarios o partes externas. A fin de asegurar un intercambio seguro de la información que reduzca los riesgos que puedan derivarse del mismo, deberán de tenerse en consideración los siguientes aspectos:

- El uso de correo electrónico y de soportes externos como medios de intercambio de información, se encontrará sujeto a las directrices y normas indicadas en los apartados correspondientes de la presente normativa.
- Desde WINDAR se habilitarán los mecanismos necesarios para posibilitar un intercambio de información seguro y eficaz tanto entre usuarios internos como con usuarios externos a la organización. Los usuarios deberán de utilizar dichos mecanismos de intercambio de información, debiendo de requerir autorización expresa en caso de que se pretenda utilizar cualquier mecanismo adicional.

⇒ En este sentido, el intercambio de información a nivel interno (entre usuarios de la organización) se realizará a través de la utilidad interna (CEDOC), a través de la estructura de carpetas de los equipos servidores de la organización, a través del correo electrónico (teniendo para ello en consideración las indicaciones realizadas en el apartado correspondiente) y los servicios cloud permitidos por la organización (OneDrive y WCloud). Adicionalmente, desde WINDAR se podrán considerar y habilitar otros mecanismos adicionales sobre los que se informará puntualmente a los usuarios.

⇒ El intercambio de información con usuarios externos se realizará a través del correo electrónico (con las limitaciones recogidas en el apartado correspondiente) y los servicios cloud permitidos por la organización (OneDrive y WCloud). Adicionalmente, desde WINDAR se podrán considerar y habilitar otros mecanismos adicionales sobre los que se informará puntualmente a los usuarios.

⇒ En el caso de que usuarios externos (clientes, proveedores, colaboradores,...) pretendan compartir información con usuarios de WINDAR por vías diferentes a las indicadas, se consultará al área de TI o a los responsables designados a tal efecto, a fin de evaluar la viabilidad de uso de dichas herramientas.

- Con carácter general, y salvo autorización expresa, no podrán instalarse y explotarse programas de almacenamiento, sincronización de archivos, discos duros virtuales o de copias de seguridad en Internet tipo Dropbox, Box, Google Drive, etc. para salvaguardar, compartir, o distribuir información y datos de la empresa o de sus clientes, o cualquier tipo de documentación propia de trabajo.
- En el caso de que la información intercambiada o facilitada a partes externas contenga datos de carácter personal o se encuentra categorizada como información confidencial o de uso restringido, deberá contemplarse la necesidad de la firma de los correspondientes compromisos de confidencialidad o contratos de tratamiento externo de datos. En caso de dudas al respecto, el usuario podrá dirigirse a los responsables designados a tal efecto, a través de la herramienta de ticketing.
- Para una adecuada protección de la información confidencial o de uso restringido, podrá ser necesaria la aplicación de medidas adicionales como pueden ser mecanismos de cifrado o canales de comunicación o intercambio con adecuados protocolos de seguridad. WINDAR habilitará a los usuarios las herramientas y mecanismos necesarios para una adecuada aplicación de esta medida.

7. Política de Control de Accesos

Como se ha indicado, los usuarios únicamente deberán de disponer de acceso a la información y a los recursos que estrictamente necesiten para el desarrollo de su actividad laboral. Desde WINDAR se han implementado los procesos y mecanismos necesarios para reducir los riesgos derivados de accesos no autorizados, excesivos o inadecuados. En este sentido se debe de considerar que:

- Cada usuario dispondrá de una cuenta personalizada, dotada de los accesos y aplicaciones exclusivamente necesarios para el correcto desarrollo de sus labores profesionales. El usuario no deberá modificar ni vulnerar los permisos procurados por la empresa, especialmente con intención de instalar aplicaciones no relacionadas con el trabajo.
- En caso necesario que el usuario estime oportuna la extensión de sus permisos o la instalación de una aplicación específica para llevar a cabo su labor, deberá solicitarlo a los responsables designados a tal efecto, a través de ticket o solicitud generada a tal efecto.
- Todo acceso a los equipos y sistemas de información estará controlado y autorizado por los administradores de sistemas o responsables designados a tal efecto. Queda estrictamente prohibido para el usuario, intentar acceder a los sistemas o recursos a los que no tenga autorización expresa por parte de estos.
- Todo usuario autorizado tiene acceso a los sistemas informáticos mediante un nombre de usuario y contraseña personal e intransferible, comprometiéndose a tratarla con la máxima diligencia y confidencialidad, siendo el único responsable del buen uso de la misma. El titular autorizado será responsable único y directo de todo lo ejecutado en el sistema bajo su nombre de usuario y contraseña. Asimismo, quedan estrictamente prohibidos los intentos reiterados, por cualquier medio, para obtener el acceso a contraseñas de otros usuarios sin su consentimiento.
- En el momento de alta en la empresa, los administradores de sistemas o responsables designados a tal efecto facilitarán al usuario de forma segura su identificador y contraseña de acceso garantizando en todo caso su confidencialidad y secreto, facilitando al usuario la posibilidad de modificar posteriormente la contraseña.
- Las contraseñas de acceso estarán sujetas a las políticas de contraseñas seguras que se definan a fin de asegurar su eficacia y su protección, incluyendo aspectos como longitud mínimo, uso de requisitos de complejidad (caracteres especiales, números, mayúsculas y minúsculas...), caducidad,....

- Con carácter general, se prohíbe divulgar por cualquier medio las claves de acceso a cualquiera de los servicios que se faciliten a los empleados., salvo, excepcionalmente y de forma justificada, a los administradores de sistemas o responsables de TI, para tareas específicas de administración y/ o resolución de incidentes. En estos casos, deberá de quedar constancia de este uso excepcional y de las actividades realizadas al respecto.
- Todos los nombres de usuario, contraseñas, claves de acceso y demás identificadores facilitados al usuario tendrán el carácter de confidencial, resultando personales e intransferibles, salvo con las excepciones indicadas anteriormente. Los usuarios se comprometen a dar aviso al administrador de sistemas y/o al responsable de seguridad de forma inmediata de cualquier incidencia o anomalía detectada en los accesos a los sistemas de información o en la seguridad de los mismos.
- Los usuarios son responsables del uso y custodia de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la empresa no debiendo comunicarlas en ningún caso a otros usuarios, ni registrarlas o escribirlas en ningún formato (ya sea soporte digital o soporte papel) salvo en aquellas herramientas específicas que se habiliten en la organización y que garanticen un almacenamiento seguro de las mismas, a fin de evitar accesos no autorizados a los sistemas, o que se pueda suplantar la identidad del usuario.
- El usuario no permitirá a terceras personas acceder a ordenadores o sistemas de WINDAR usando sus credenciales, excepto cuando sea explícitamente autorizado por WINDAR para la resolución de algún problema.
- Cada vez que termine su jornada laboral, o se ausente de su puesto de trabajo, el usuario se encargará de bloquear o cerrar su sesión en los ordenadores y sistemas de WINDAR a los que se encuentre conectado.
- Se realizarán, por parte de los Responsables designados a tal efecto, revisiones periódicas y programadas de los derechos de acceso, privilegios o permisos de los usuarios verificando que estos disponen de acceso a las utilidades, y recursos o sistemas que precisan para el desarrollo de sus funciones, y que se cumple el principio de "mínimo privilegio" QUE HAGAN ALGO.

8. Política de uso de correo electrónico

El correo electrónico es una herramienta que la empresa habilita para aquellas comunicaciones requeridas como consecuencia del desarrollo de la actividad propia de la empresa con otras entidades o con otros usuarios. El acceso y uso de estos servicios por parte de los usuarios, así como los privilegios asociados a dicho derecho, deben limitarse a los establecidos por sus obligaciones profesionales. WINDAR, consciente de los problemas de seguridad y responsabilidad legal que ocasiona el uso del correo electrónico, dispone las siguientes normas:

- El correo electrónico de empresa, las listas de distribución, los servicios de mensajería instantánea y demás servicios de comunicación electrónica, son herramientas cuyo objetivo principal es facilitar la comunicación corporativa exclusivamente en el ámbito laboral.
- Los usuarios serán responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la empresa. Los usuarios deberán ser conscientes de los riesgos que conlleva los usos indebidos de las direcciones de correo electrónico suministrados por la empresa y las posibles repercusiones (como daños a la imagen de la empresa) que podría provocar una utilización inadecuada de dichos recursos.

- No deben utilizarse las herramientas de comunicación para uso personal, ni se podrán utilizar cuentas de correo personales, basadas en acceso a web, tipo gmail, hotmail. Excepcionalmente, podrá usarse sólo cuando la situación esté debidamente justificada y no contravenga en modo alguno los intereses de la empresa. En este caso el acceso deberá ser exclusivamente a aquellos correos que sean de plena confianza, y en ningún caso deben abrirse enlaces o descargarse ficheros adjuntos en el ordenador del usuario o de otros usuarios, aunque provengan de personas conocidas, para evitar así la intrusión de virus o código malicioso.
- Está terminantemente prohibido el reenvío de correos y la documentación propia de trabajo a cuentas de correo electrónico personales, o que no se encuentren bajo control directo de la empresa, así como la redirección, importación o descarga del correo electrónico corporativo en otros gestores o plataformas de correo web tipo Gmail, Hotmail, etc.
- La forma y contenidos de los correos enviados por el usuario estarán alineados con las normas éticas y de cortesía marcadas por la empresa, y en ningún caso se enviarán correos electrónicos con mensajes ofensivos, amenazantes, de mal gusto, con contenido ilícito o fraudulento. Todos los mensajes enviados por correo electrónico corporativo deberán de incluir los avisos legales, formato, información de contacto, y demás información que componga los modelos de firmas de los correos corporativos que se le indique a los usuarios por parte de los responsables designados durante el proceso de alta en la empresa.
- Queda prohibido la utilización del correo electrónico con fines lucrativos o comerciales, para uso recreativo o cualquier otro que no guarde relación con la actividad laboral, o que sean ajenos al propio desarrollo de las actividades de la empresa.
- Se prohíbe el uso del correo profesional para la inscripción a “newsletter”, grupos de noticias, o similares que no estén directamente relacionadas con la actividad profesional desarrollada por el usuario y que resulten de plena confianza.
- Las listas de distribución de correo solo podrán ser utilizadas para los fines propios de la empresa, y nunca con fines publicitarios, comerciales o de índole personal que no vayan relacionadas con actividades propias del desempeño laboral.
- No se divulgarán, independientemente del formato en que se encuentren, correos que revelen datos del directorio o de usuarios pertenecientes a la empresa, fuera de los límites laborales establecidos por la misma.
- La cuenta de correo personal corporativa y la firma corporativa serán las únicas autorizadas para su uso en la comunicación personal con terceros (clientes, proveedores, partners...etc.).
- Los usuarios deberán revisar con debida diligencia la barra de direcciones antes de enviar un mensaje. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información. Cuando se responde a un mensaje es importante revisar las direcciones que aparecen en el campo Con Copia (CC).
- No se deben enviar o reenviar correos de forma masiva. Si se envía un correo a un conjunto de destinatarios, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Copia Oculta (CCO), evitando su visibilidad a todos los receptores del mensaje.
- No enviar mensajes en cadena. Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe proceder a su borrado inmediatamente.
- No responder a mensajes de Spam. La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envía a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a la Organización. En cualquier caso, nunca deben de responderse.
- Con carácter general, no está autorizado el envío de correos que contengan en el cuerpo o en los adjuntos información con datos confidenciales o de uso restringido, debiendo de priorizar el uso de otro tipo de herramientas disponibles en la organización (indicadas en el apartado de Intercambio de Información del presente documento). En caso de que sea necesario el envío de esta información deberá ponerse en contacto con los responsables designados a tal efecto, a través de la herramienta de ticketing, quienes le proporcionará mecanismos alternativos para su realización
- Asegurar la identidad del remitente antes de abrir un mensaje. Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) de la persona atacada. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información confidencial o de uso restringido a petición de un correo del que no se puede asegurar la identidad del remitente debe rechazarse. Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).
- No abrir correos basura ni correos sospechosos. Aun cuando un mensaje no deseado hubiera traspasado el filtro contra spam, no debe abrirse, debiendo reportarse el correspondiente incidente de seguridad. Es conveniente borrar los correos sospechosos o, al menos, situarlos (sin abrir) en una zona de cuarentena.
- No ejecutar archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin que estos se analicen previamente con las herramientas contra código malicioso disponibles en la organización, las cuales se configurarán de modo que realicen este análisis de forma automática. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).
- Informar de correos con virus, sin reenviarlos. Si el personal detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente de seguridad al área IT y no reenviarlo, para evitar su posible propagación.
- No utilizar el correo electrónico como espacio de almacenamiento. La capacidad de espacio en los servidores de correo es limitada. Cuando una cuenta se satura puede ser que se restrinjan por parte del servidor los privilegios de envío y/o recepción de mensajes o que se realice un borrado, más o menos selectivo, de los mensajes almacenados. Por todo ello, se recomienda conservar únicamente los mensajes imprescindibles y revisar periódicamente aquellos que hubieren quedado obsoletos. En este sentido, desde la organización se desarrollarán normas y políticas de eliminación de información, que serán comunicadas a los usuarios para su consideración y aplicación.
- WINDAR, se reserva el derecho de acceder y monitorizar el uso de este y cualquier otro recurso facilitado a los usuarios, siempre y cuando este acceso se encuentra legitimado o justificado para asegurar la continuidad de las operaciones y la prestación de los servicios de la sociedad, garantizar o supervisar la seguridad de la información y la aplicación de los procedimientos definidos al respecto, o asegurar el desempeño de los trabajadores, siempre teniendo en cuenta lo establecido en el Estatuto de los trabajadores y en el resto de legislación de aplicación, y según lo indicado en el apartado correspondiente de la presente normativa.

9. Política de uso de Soportes Externos

El uso de soportes externos, como pueden ser memorias USB, discos duros externos, CD/DVD,... puede ser necesario en la organización para la realización de determinadas tareas como puede ser el traslado de información o su intercambio con clientes u otras partes, respaldo de información, intercambio de información entre áreas... Sin embargo, su uso no controlado puede introducir riesgos de seguridad de la información como pueden ser dispersión y pérdida de control de la información, pérdida de información, acceso no autorizado, introducción de virus en los sistemas de la organización... Por ello, desde WINDAR se han definido las siguientes normas de uso que deben ser aplicadas por todos los usuarios de la organización que utilicen o pueden utilizar soportes externos:

- Con carácter general, el uso de soportes externos por parte de los usuarios se encuentra prohibido salvo que se disponga de autorización expresa por parte de los responsables designados a tal efecto, para su uso con finalidades concretas asociadas a su actividad laboral, como puede ser el intercambio de información con clientes o usuarios internos. En este sentido, se tratará de priorizar otras herramientas disponibles en la organización para el intercambio de información como pueden ser los indicados en el apartado correspondiente de la presente normativa.
- En todo caso, el uso de soportes se limitará a fines profesionales, quedando prohibido su uso o conexión a los sistemas de la organización para fines personales u otros tipos de fines.
- La autorización para el uso de soportes se gestionará través de la herramienta de ticketing habilitada a tal efecto, y se realizará por los responsables designados a tal efecto (responsables de área), bajo la supervisión de los responsables de TI, quienes se encargarán de gestionar la custodia y asignación de los soportes autorizados, manteniendo los correspondientes inventarios de soportes y registros de asignación de los mismos.
- Únicamente se autoriza el uso de soportes corporativos, gestionados y controlados por los responsables correspondientes de la organización. Se prohíbe el uso de soportes extraíbles personales o no controlados por la organización.
- El uso de soportes externos facilitados por clientes, colaboradores, proveedores y otras terceras partes para intercambiar información con WINDAR, deberá de quedar igualmente supeditado a la autorización y supervisión de los responsables designados a tal efecto y del personal de TI, quienes se encargarán de validar y autorizar su uso y de evaluar los riesgos que estos puedan introducir sobre los sistemas de WINDAR.
- Una vez que los usuarios finalicen las tareas para las cuales requirieron el uso de soportes, estos serán devueltos a los responsables correspondientes para que se proceda a la eliminación segura de la información contenida en los mismos y la verificación de que estos se encuentran libres de código malicioso.
- Con carácter general, y, especialmente, en el caso de que se almacene en los mismos información confidencial o de uso interno, los soportes externos deberán de ser cifrados a través de los mecanismos que la organización habilitará a tal efecto.
- La organización podrá implementar las medidas técnicas necesarias para monitorizar el uso de soportes extraíbles y/o para limitar y bloquear su uso según las necesidades de la organización y a fin de garantizar la seguridad de la información propia o de nuestros clientes.
- Durante su uso, los usuarios deberán de aplicar, en la medida de sus posibilidades, las buenas prácticas y usos necesarios para evitar incidencias que afecten a la seguridad de la información como pueden ser accesos no autorizados, pérdidas de información, introducción de virus y código malicioso...

- En caso de que los usuarios sufran o detecten cualquier incidencia relacionada con el uso de soportes, o con el cumplimiento de la presente normativa, deberá de notificarlo al área de TI a través de los mecanismos de notificación de incidencias establecido.

10. Uso responsable de internet. Restricciones a la navegación

Internet es un servicio que WINDAR pone a disposición de su personal para uso estrictamente profesional. La empresa es consciente que la introducción de Internet en el ámbito laboral aumenta las amenazas a la seguridad de la red, afecta a la productividad de los empleados y disminuye el ancho de banda disponible. Por tanto, se considera obligada a establecer las siguientes reglas que se deben aplicar durante su uso:

- Queda prohibida la utilización de la red para navegar por sitios de Internet para otros usos que no sean los permitidos para el desempeño de su actividad laboral, salvo autorización expresa a tal efecto.
- Los usuarios son los únicos responsables de las sesiones iniciadas en internet desde sus terminales de trabajo, y se comprometen a cumplir las reglas y normas de funcionamiento establecidas en el presente documento.
- La navegación por sitios web, el envío de mensajes, registros, altas, relleno de formularios y cualquier otra actividad realizada vía Internet, serán completa responsabilidad del usuario emisor y en todo caso deberá asumir las consecuencias que emanen de su actuación.
- En caso de dudas respecto a los posibles usos de navegación y los aspectos indicados anteriormente, puede dirigirse al área de soportes a través del correspondiente ticket o solicitud de soporte.
- El acceso al servicio de Internet de la empresa por personal externo se realizará de manera controlada y autorizada, debiendo de seguirse al respecto lo definido a través del proceso de gestión de visitas que se defina al respecto.
- La empresa se reserva el derecho a filtrar el contenido al que el usuario pueda acceder a través de Internet desde los recursos y servicios propiedad de WINDAR, así como a monitorizar y registrar los accesos realizados desde los mismos.
- En caso de que los usuarios requieran el acceso a servicios web que se encuentran bloqueados o limitados por la organización, se deberá recabar la correspondiente autorización de los responsables de área, y se deberá de generar la correspondiente solicitud al área de TI, a través de la herramienta de ticketing habilitada a tal fin., quienes evaluarán la viabilidad y posibilidad de facilitar el acceso en función de las necesidades del usuario y la organización, y los riesgos que puedan derivarse al respecto.
- Está estrictamente prohibido el acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilícitos, dañinos, material pornográfico, de contenido xenófobo, racista, sexual, o cualquier material inadecuado o que atente contra la dignidad y los principios éticos y morales, y, en general, de todo tipo de contenidos que incumplan las normas de cortesía de la empresa.
- Tampoco se permite el almacenamiento en los equipos de archivos y contenidos personales descargados vía Internet, especialmente aquellos que violen la legislación vigente relativa a la propiedad intelectual. Los usuarios deberán respetar y cumplir las disposiciones legales de derechos de propiedad intelectual.

11. Uso de las licencias de software

El software o aplicaciones utilizado por la organización, así como otros recursos de información, pueden estar protegidos por la propiedad intelectual, o disponer de copyrights o derechos de autor. Desde WINDAR se dispone de las herramientas y sistemáticas necesarias para asegurar el cumplimiento efectivo de estos requisitos. En este sentido, los usuarios deberán de considerar que:

- Los usuarios están obligados a respetar las condiciones de licencia y copyright del software instalado en los equipos informáticos, siendo responsables de su adecuada utilización.
- Todo software protegido por copyrights o derechos de autor no podrá ser copiado, ni se podrá disponer de cualquier información protegida por los derechos de autor que esté en formato electrónico en el equipo de cualquiera de los usuarios.
- Los usuarios no podrán instalar o descargar software sin la previa autorización de los responsables designados a tal efecto, quienes deberán de asegurar un correcto cumplimiento de la legislación relacionada con la propiedad intelectual. Únicamente se podrá instalar software en los sistemas de la organización que esté debidamente autorizado y que cumpla con los requisitos de la Ley de Propiedad Intelectual.
- Los usuarios serán responsables de todo software instalado en sus equipos sin autorización expresa por los responsables designados a tal efecto, así como de uso y en su caso, de los daños que causen a los equipos o sistemas de información que deriven de su uso o instalación.
- Cualquier actividad que infrinja las leyes de la propiedad intelectual, incluyendo los derechos de autor, marcas o derechos registrados y el de su reproducción será sancionado según lo indicado en la presente normativa.

12. Tratamiento de datos de carácter personal

WINDAR ha implementado los mecanismos necesarios para asegurar un adecuado cumplimiento de la normativa de protección de datos personales. Con carácter general la organización proporcionará a los usuarios las herramientas y procedimientos necesarios para asegurar un cumplimiento efectivo de dicha normativa. Sin embargo, pueden darse durante la interacción con clientes, proveedores, colaboradores y otras partes interesadas, situaciones en las que la participación de los usuarios o trabajadores de WINDAR sean necesarias. En este sentido, WINDAR ha designado responsables específicos relacionados con el cumplimiento de la normativa de protección de datos (en particular se ha designado un Delegado de Protección de Datos) que se encuentran a disposición de los trabajadores de la organización para orientar, asesorar o aclarar las dudas que puedan surgir respecto al cumplimiento de los requisitos de la normativa. En este sentido, los usuarios deben conocer que:

- El tratamiento de datos personales debe responder a una finalidad legítima y concreta, como puede ser, en general, el mantenimiento de una relación contractual (como puede ser la mantenida con los clientes).
- Los datos personales utilizados durante el desarrollo de los servicios internos o externos deberá de ser proporcional a la finalidad del tratamiento, no debiendo de utilizarse más datos de aquellos que sean estrictamente necesarios para cumplir con dicha finalidad.
- Los titulares de los datos tienen derecho a ser informados respecto al tratamiento de sus datos, así como al posterior acceso a los mismos, y a su cancelación, rectificación, oposición, portabilidad o limitación del tratamiento. En caso de que algún afectado se dirija directamente a los usuarios de la organización para el ejercicio de los derechos indicados, el usuario deberá de trasladar, con la mayor celeridad posible, dicha solicitud a los responsables designados a tal efecto.

- Los datos de carácter personal deberán de ser adecuadamente protegidos, para lo cual serán de aplicación, entre otras, las medidas indicadas en la presente normativa. Adicionalmente, en función del tipo de datos y de la finalidad del tratamiento, podrá ser necesaria la aplicación de medidas adicionales como pueden ser la aplicación de mecanismos de cifrado, seudonimización o anonimización de datos, para lo cual desde WINDAR se habilitarán las herramientas y mecanismos necesarios.
- Las incidencias o brechas de seguridad que afecten a datos de carácter personal deberán de ser notificadas (según los mecanismos habilitados a tal efecto) con la máxima celeridad posible, a fin de poder dar respuesta a los requisitos de la normativa al respecto.
- El acceso a datos personales por parte de terceros debe de quedar regulado a través de los correspondientes contratos de tratamiento externo de datos. Desde WINDAR se dispone de los procedimientos adecuados para el establecimiento de dichos acuerdos, si bien los usuarios, cuando pretendan realizar un intercambio o envío de información que contenga datos de carácter personal, deberán de consultar y verificar la existencia de dichos acuerdos, solicitando o consultando al área de Protección de Datos de Windar a través de los medios de contacto habilitados a tal efecto.

13. Gestión de incidencias

Todas las incidencias en la utilización de los recursos y medios tecnológicos de la empresa, o que, por cualquier circunstancia, directa o indirecta pueda comprometer la Seguridad de la Información, deberá ser notificada con la mayor brevedad que sea posible a través de los medios habilitados a tal efecto.

En este sentido, en WINDAR se dispone de una herramienta de ticketing (GLPI) a través de la cual, entre otros aspectos, se gestionan las incidencias que afectan a la seguridad de la información, a los sistemas de tratamiento y a la a los recursos TIC.

Con carácter general, los usuarios deberán de priorizar el uso de esta herramienta para la notificación de las incidencias, si bien, excepcionalmente, y especialmente en caso de que no se disponga de acceso a dicha herramienta, se podrán notificar las incidencias por correo electrónico o por vía telefónica, dirigiéndose a los responsables designados a tal efecto.

En la notificación del incidente, el usuario deberá de trasladar toda la información que le sea posible del mismo, tratando de indicar aspectos como: la descripción del incidente, el origen del mismo, los activos afectados, la información afectada, así como otra información que pueda considerar relevante.

Desde WINDAR se han designado a los responsables y personal especializado necesarios para una adecuada gestión de las incidencias tras su notificación, quienes serán los encargados de realizar el diagnóstico, seguimiento y resolución, manteniendo durante todo el proceso actualizado el registro de incidencias, y, en los casos necesarios, manteniendo informado a los usuarios al respecto. Durante este proceso, es posible que los responsables y técnicos designados, requieran información adicional al usuario a fin de tratar de optimizar la resolución de la misma.

14. Uso de teléfonos móviles corporativos

WINDAR, con objeto de optimizar y facilitar el trabajo de sus empleados ofrece soluciones de telefonía y datos a los usuarios que, por sus competencias, así lo necesitan. Sin embargo, el uso fraudulento del teléfono, fijo o móvil, puede poner en peligro la integridad de la empresa y lesionar sus intereses. Esto puede acontecer mediante la práctica de actividades consideradas ilícitas, que atenten contra la ética o moral o puedan resultar ofensivas, o incluso como consecuencia del uso abusivo del mismo.

Los teléfonos móviles y los módems de datos USB 3/4G son asignados a los usuarios y colaboradores de WINDAR que en el ámbito de su actividad profesional necesiten realizar o recibir contactos frecuentes y regulares con clientes, proveedores, colaboradores y coordinadores, o deban desplazarse fuera de las oficinas permanentes de la compañía, y/o deban estar localizados por razón de su trabajo (comercial, consultoría, mantenimiento, etc.)

Cada director de área operativa, proyecto o servicio, debe determinar el interés en la utilización por parte del respectivo colaborador de un teléfono móvil, smartphone o modem de datos USB 3/4G. En caso de que sea la propuesta sea aprobada por la dirección de WINDAR, el director del área operativa solicitará a los responsables designados a tal efecto el comienzo de los trámites para la contratación del equipamiento necesario.

Las condiciones generales de utilización de dicho servicio son las siguientes:

- Los teléfonos móviles, smartphone, modems de datos USB 3/4G, facilitados por la organización, así como todos sus accesorios, y el contrato de servicio de red correspondiente, son propiedad de la WINDAR y su uso deberá ajustarse a las normas indicadas en el presente documento, así como en otras políticas o normativas que se desarrollen a tal efecto
- Por razones logísticas y de control, el contrato del operador de red correspondiente es nominal a WINDAR.
- El uso personal de las comunicaciones telefónicas estará permitido si es fortuito o insignificante, y no interfiere en las actividades laborales habituales ni perjudica el rendimiento de las mismas.
- En caso de baja de un colaborador/empleo en la compañía, este deberá devolver el terminal, incluido sus embalajes originales, en perfectas condiciones de utilización, pudiendo tener la posibilidad de adquirir el terminal por su valor residual, si procede. Una vez devuelto el dispositivo, desde WINDAR se procederá a la eliminación de todos los datos e información del celular (incluyendo la agenda de contactos, fotos, mensajes, etc.) a fin de posibilitar su reasignación o su retirada segura.
- El uso profesional del equipo de teléfono móvil se enfocará a la mejor calidad de atención a nuestros clientes, a la mejora de la calidad de reacción, y por tanto al aumento de productividad del colaborador de WINDAR..
- Es responsabilidad del colaborador de WINDAR hacer el mejor uso profesional del equipo de telefonía móvil.
- WINDAR no financiará en ningún caso la compra de accesorios (kits de manos libres, fundas, kits para transmisión de datos, etc.) ni tampoco su instalación. El colaborador se hace directamente responsable del deterioro que se pudiera producir en el terminal asignado por la utilización de dichos accesorios.
- WINDAR podrá solicitar en cualquier momento la devolución del terminal en su totalidad, o en parte, al colaborador, quien deberá restituirlo en perfecto estado de conservación.

WINDAR se reserva el derecho de revisar la lista de llamadas de voz y datos cursadas, para la verificación del cumplimiento y seguimiento de las normas ante cualquier sospecha fundada o evidencia de uso fraudulento o abusivo del servicio, así como de retirar el derecho a la utilización del teléfono móvil/modem de datos en caso de utilización inapropiada, abusiva, y/o que produzca perjuicios a la empresa.

La empresa se reserva el derecho de modificar el presente reglamento como el ámbito de aplicación del mismo, previa comunicación a sus colaboradores.

15. Organización de la Seguridad de la Información

En WINDAR se han definido las responsabilidades necesarias para una adecuada gestión de la seguridad de la información, así como, en particular, para asegurar un desempeño eficaz de los aspectos definidos en la presente normativa. En particular, en WINDAR se ha habilitado un Comité de Seguridad de la Información con la responsabilidad de coordinar, centralizar y gestionar los procesos necesarios para una adecuada gestión de la seguridad de la información y la toma de decisiones al respecto.

En relación a lo indicado en la presente normativa, el Comité de Seguridad se encuentra a disposición de los usuarios para ofrecer el apoyo y asesoramiento necesario para los aspectos indicados en la presente normativa, incluyendo aquellos aspectos para cuyo cumplimiento los usuarios requieran aclaración u orientación adicional.

La comunicación con el Comité de Seguridad se realizará, con carácter general, a través de la herramienta de ticketing (GLPI) donde se ha establecido una categorización específica para los aspectos relacionados con la seguridad de la información.

En particular, los responsables que componen el Comité de Seguridad, y que se encuentran a disposición de los usuarios para ofrecer el apoyo y asesoramiento necesario son:

- ⇒ Raúl González, Responsable del Sistema de Gestión
- ⇒ Covadonga Carballo, Directora de Technology and Innovation
- ⇒ Fernando Ruiz, Responsable de TI
- ⇒ Oier Zurimendi Unzueta, Delegado de Protección de Datos (DPO)

Por otro lado, desde WINDAR se desarrollarán las actividades de sensibilización y formación necesarias para asegurar que todos los usuarios de la organización disponen de un nivel de concienciación y capacitación en materia de seguridad de la información adecuado a las necesidades asociadas a su puesto o perfil laboral, a fin de reducir los riesgos de seguridad de la información que puedan derivarse de sus actividades.

Estas acciones de formación y sensibilización se regirán según lo definido en el procedimiento de formación, e irán orientadas al cumplimiento de, entre otros, los siguientes objetivos:

- Adaptación a nuevas tecnologías y nuevos sistemas de trabajo
- Incremento de la calificación del personal
- Cumplimiento de las normas y políticas definidas por la organización
- La importancia de la conformidad con la política, los procedimientos y requisitos de seguridad de la información y calidad del software,
- Los riesgos de seguridad de la información asociados con su trabajo,
- Sus funciones y responsabilidades en el logro de la conformidad con los requisitos de seguridad,
- Las consecuencias potenciales de desviarse de los procedimientos que les sean de aplicación,
- La importancia de su participación en el proceso de mejora continua del Sistema de gestión de seguridad de la información y de calidad del software.
- La importancia del deber de secreto y el compromiso de confidencialidad asumido.

Estas acciones de formación y sensibilización podrán incluir, entre otras actividades:

- La comunicación de políticas y normativas de seguridad,
- Acciones formativas específicas internas o externas,
- Charlas de sensibilización internas,
- Comunicaciones por correo electrónico, intranet u otras vías de comunicación de buenas prácticas de seguridad de la información o de información sobre vulnerabilidades de los sistemas y amenazas que puedan afectarle,
- El desarrollo de ejercicios de phishing controlado o simulado,
- El desarrollo de tests o encuestas que permitan evaluar por parte de la organización el grado de sensibilización y concienciación en materia de seguridad de la información.

16. Programas y dispositivos de control y monitorización

WINDAR ha puesto en funcionamiento herramientas y servicios de control automatizadas para analizar y detectar aquellos eventos que puedan suponer riesgos para la seguridad de la información y los sistemas o identificar los usos y comportamientos indebidos o ilícitos en la red, no implicado dicho control violación a la privacidad o a la intimidad de los usuarios, y realizándose, en todo caso, respetando los derechos recogidos en la normativa laboral (Estatuto de los Trabajadores).

Desde WINDAR se informa que, por cuestiones de seguridad toda la información que circula por la red, así como por el correo electrónico de las cuentas administradas por la empresa, podrá ser monitoreada y sujeta a controles y reportes sobre su uso, brindando información como: usuario, fecha de accesos, hora de accesos, bytes transferidos, almacenamiento de ficheros, acceso a los servidores, sitios visitados, tiempo de navegación por la red, entre otros.

17. Uso de la inteligencia artificial

WINDAR ha autorizado como asistente de inteligencia artificial en el entorno corporativo Microsoft COPILOT. El resto de asistentes disponibles en el mercado, como ChatGPT, Gemini IA u otros, no están autorizados para su uso en el entorno de trabajo corporativo. La regulación del uso de este tipo de herramientas trae causa, principalmente, de los riesgos que conlleva su uso para con la confidencialidad de la información, así como la salvaguarda de los derechos relativos a los datos personales.

- Entono corporativo hace referencia al ámbito interno de trabajo dentro de las sociedades y emplazamientos de Grupo WINDAR. Se caracteriza por el uso de Microsoft COPILOT como asistente de IA mediante la adquisición de licencia oficial de Microsoft, de forma que se integra con las herramientas de Office 365 mejorando la productividad de los usuarios y garantizando mayor seguridad y privacidad al utilizar documentos propios y ajenos.

El uso del entorno corporativo solo estará disponible a los usuarios habilitados por los responsables de cada área o departamento. Para ello, deberán de solicitar previamente al área de IT, la licencia correspondiente.

- El entono NO corporativo hace referencia al uso de COPILOT así como de otros asistentes de inteligencia artificial como ChatGPT, Gemini IA u otros en abierto, a través del navegador de internet. El uso de datos e información corporativa propiedad de WINDAR, así como, la información propiedad de clientes o terceros a través de estas herramientas de IA, está totalmente prohibido.

La seguridad y la privacidad son aspectos cruciales en la implementación y uso de asistentes de inteligencia artificial (IA). Por esta razón, todas las personas de las sociedades y emplazamientos WINDAR que utilicen los asistentes de inteligencia artificial garantizarán el cumplimiento de las siguientes normas:

- Serán conscientes de que están comunicándose o interactuando con sistemas de inteligencia artificial, por lo que se responsabilizarán del uso apropiado y adecuado de los asistentes de IA.
- Utilizarán en todo momento los asistentes de IA que han sido autorizados por WINDAR y exclusivamente como ayuda a las en la realización de sus funciones y tareas, respetando en todo momento la reglamentación, normas y pautas internas establecidas por la compañía.
- Adoptarán siempre principios de transparencia y equidad, garantizando en todo momento, un uso justo y beneficioso de los asistentes de IA y de los resultados proporcionados por la IA.
- Actuarán con responsabilidad a la hora de utilizar los asistentes de IA aplicando en todo momento las mejores prácticas disponibles para minimizar los riesgos asociados a la automatización de las tareas y resultados.
- Garantizarán la privacidad y seguridad de los datos e información empleada para alimentar a los asistentes de IA. En ningún caso, se suministrará a la IA acceso a información sensible y personal. Asegurarán la exactitud y veracidad de los datos e información proporcionada validando la misma previamente a su uso.
- Revisarán los resultados con precaución, especialmente en el caso de que los datos e información sean empleados para la toma de decisiones.
- Monitorizarán las respuestas proporcionadas por la IA para identificar y mitigar posibles sesgos en los resultados generados, en muchas ocasiones debidos a la propia información que le es proporcionada por él usuario.
- Interpretarán los resultados proporcionados por la IA dentro del marco de sus funciones y tareas particulares y cuando sea necesario los complementarán con su propio conocimiento o información adicional.
- Nunca se delegará la responsabilidad de las personas en los asistentes de IA a la hora de crear resúmenes, documentos o el análisis de datos. Es responsabilidad de todas las personas de WINDAR comprobar los resultados y enriquecerlos definitivamente con sus aportaciones.
- Comprenderán el funcionamiento de los asistentes de IA, las fuentes de datos a utilizar y las limitaciones en su uso. Se cumplirá siempre con los controles y políticas establecidas internamente para supervisar su uso. Se evitará que se tomen decisiones automatizadas sin supervisión humana.

El departamento de IT podrá realizar auditorías y monitorizaciones periódicas del uso de la IA con el objeto de detectar de forma temprana el uso indebido de los sistemas de IA, que podrán desencadenar en una sanción disciplinaria, dentro del marco regulatorio aplicable, en su caso.

18. Responsabilidades derivadas del incumplimiento de la normativa

El presente documento estará regulado por las leyes y normativa española, así como las que dimanen de la Unión Europea y de las comunidades autónomas en relación con protección de datos de carácter personal, propiedad intelectual y uso de herramientas telemáticas, así como la normativa aplicable dentro del ámbito laboral y toda la que pueda aparecer en un futuro.

El usuario debe ser consciente de que el incumplimiento de esta normativa de seguridad puede causar daños relevantes a la organización, y suponer una violación de su compromiso de confidencialidad adquirido como empleado o usuario de WINDAR.

Los usuarios se comprometen al cumplimiento de la misma, en la medida de sus posibilidades, así como a comunicar a los responsables definidos a tal efecto, en caso de detectar o prever cualquier incumplimiento al respecto. WINDAR podrá hacer responsable al usuario de las consecuencias derivadas por el incumplimiento de las normas establecidas en este documento.

La empresa se reserva el derecho de evaluar periódicamente el cumplimiento de este reglamento (incluyendo mediante el uso de herramientas y servicios de control, auditoría y monitorización automatizadas, para analizar y detectar aquellos eventos que puedan suponer riesgos para la seguridad de la información y los sistemas o identificar los usos y comportamientos indebidos o ilícitos en la red), y de aplicar las medidas disciplinarias y legales que estime oportuno como consecuencia del incumplimiento de la misma.

En caso de detectarse alguna acción contraria a lo dispuesto en la presente normativa de seguridad de la organización o, en último caso, una brecha de seguridad, WINDAR puede ordenar una investigación para determinar el tipo de falta cometida, evaluando la situación teniendo en cuenta los siguientes factores:

1. La naturaleza y la gravedad de la infracción.
2. El impacto de la infracción en las actividades de la organización.
3. El nivel de incumplimiento respecto a la normativa de seguridad y a la cultura de la organización.
4. La reiteración de los hechos probados.
5. La destreza y los conocimientos del trabajador.
6. Otros factores legales aplicables.

La determinación de la gravedad de la falta tendrá en consideración estos factores, así como lo definido en el Convenio Colectivo, el Estatuto de los Trabajadores, y el resto de legislación que pueda ser de aplicación.

En caso de determinarse que se trata de una falta leve, de acuerdo con la regulación disciplinaria legal o convencional aplicable, se tomarán las medidas adecuadas para corregir la situación, esto es, se formará al trabajador y se le proporcionarán recursos adicionales para desarrollar las habilidades necesarias y evitar faltas futuras, monitorizando su progreso para asegurarse de que las medidas correctivas sean efectivas.

En caso de reincidir en la falta, se tomarán medidas de advertencia notificando al trabajador la falta cometida y recordándole las medidas correctivas a seguir; si la falta persiste, se considerará falta grave de acuerdo con la regulación disciplinaria legal o convencional aplicable, y se aplicará el régimen disciplinario legal o convencional de forma acorde con la mayor gravedad de la infracción.

Si el incumplimiento se considera una falta grave, o muy grave, desde WINDAR se podrá solicitar la retirada de todos los accesos a los sistemas de información e instalaciones, así como la devolución de los activos asignados. Adicionalmente, se dará traslado a las áreas correspondientes de WINDAR para proceder a la valoración de la aplicación del régimen disciplinario legal o convencional de forma acorde con la mayor gravedad de la infracción, incluyendo entre las posibles sanciones la suspensión temporal de empleo y sueldo o el despido disciplinario, dependiendo de la gravedad de la infracción. Si bien, como se ha indicado, la determinación de la gravedad de la falta requerirá del análisis desde WINDAR de los diferentes factores indicados, a modo orientativo y sin perjuicio de la regulación disciplinaria legal o convencional aplicable, se puede considerar que, en general:

- ⇒ Tendrán la consideración de Falta Leve, la no aplicación o incumplimiento de las directrices definidas en la Normativa de seguridad, salvo que este incumplimiento se realice de manera reiterada o consciente, y se pueda considerar como un acto de desobediencia susceptible de ser calificado como falta grave o muy grave.
- ⇒ Tendrán la consideración de Falta Grave, la reiteración de Faltas leves, así como el incumplimiento, de manera deliberada, de los Usos prohibidos, ilegales o no aceptables definidos expresamente en el apartado 4 de la presente Normativa.
- ⇒ Tendrán la consideración de Falta Muy Grave, aquellas faltas graves que se realicen de manera reiterada o se puedan considerar un claro acto de indisciplina o de transgresión de la buena fe contractual, o busquen causar de manera deliberada un daño a los sistemas de la organización, sin perjuicio de lo que resulte de la aplicación del régimen disciplinario legal o convencional aplicable con carácter general en la tipificación de faltas muy graves.