Política de seguridad de la información para terceras partes

Objetivo

El objeto de esta política es establecer los requisitos de seguridad de la información para las terceras partes del Grupo Zelestra que puedan acceder a información, sistemas de información, activos en operación o recursos de la organización durante su relación con la compañía.

En este sentido, las terceras partes a las que se les proporciona este documento de seguridad tienen la responsabilidad de comunicarlo a su personal asignado a Zelestra y obtener su compromiso por escrito. La política refleja requisitos legales y éticos, tanto para las actividades informales de los empleados de las terceras partes que trabajan para Zelestra, como para la realización de sus operaciones.

Los proveedores y terceros que presten servicios o suministros a Zelestra deberán cumplir con las medidas de seguridad que se especifiquen en este documento.

Prestación de servicios o suministros

Las terceras partes solo podrán realizar actividades para Zelestra que estén cubiertas por el respectivo contrato de prestación de servicios o suministros. Las actividades realizadas por el personal de las empresas proveedoras se llevarán a cabo de acuerdo con lo establecido en el contrato de provisión de servicios o suministro correspondiente, así como con las normas y procedimientos establecidos entre Zelestra y el proveedor respectivo.

Todo el personal externo que trabaje para Zelestra deberá cumplir con las políticas de seguridad de la organización. En caso de incumplimiento de alguna de estas obligaciones, Zelestra se reserva el derecho de vetar al personal que haya cometido la infracción, así como de aplicar las sanciones correspondientes en relación con la empresa contratada, que incluso podrían llevar a la rescisión de los contratos vigentes con dicha empresa.

La empresa proveedora deberá asegurarse de que todo su personal reciba la formación y capacitación adecuadas para llevar a cabo el servicio proporcionado, tanto en términos específicos relacionados con la actividad asociada a la prestación del servicio, como en términos generales de seguridad de la información. Para ello, la empresa proveedora deberá garantizar, al menos, que todo el personal involucrado en el servicio o suministro conozca y se comprometa a cumplir las políticas de seguridad establecidas.

Cualquier intercambio de información entre Zelestra y las empresas proveedoras se entenderá que se realiza dentro del marco establecido por el contrato de provisión de servicios correspondiente. Por lo tanto, dicha información no podrá utilizarse fuera de dicho marco ni para fines diferentes a los asociados con dicho contrato.

De manera general, los activos incluyen toda forma de información, así como las personas y la tecnología que respaldan los procesos de información/operación.

En cualquier diseño de proyecto o sistema, así como en el suministro de equipos de comunicación o su configuración, se debe contemplar los requerimientos mínimos de ciberseguridad anexados a contrato.

Confidencialidad de la información

El personal externo que tenga acceso a información de Zelestra deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella a la que el proveedor haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por Zelestra. Por ello:

Se evitará la revelación, modificación y destrucción no autorizada, o mal uso de la información cualquiera que sea el soporte en que se encuentre contenida.

La información confidencial no será transmitida al exterior sin la debida autorización y se mantendrá en estricta confidencialidad.

Se minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.

La presente Política fue aprobada por el Chief Digital Officer, miembro del Comité de Dirección, el 03 de diciembre de 2024 y es efectiva desde su aprobación.

En relación con la utilización de agendas de contactos, el personal únicamente introducirá datos personales como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica y teléfono profesional.

Ningún colaborador en proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada por Zelestra.

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

El empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación con Zelestra de su empresa. La utilización continuada de la información en cualquier formato o soporte distinta a la pactada y sin conocimiento de Zelestra no supondrá, en ningún caso, una modificación de este punto.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle. El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, que puede dar derecho a exigir compensaciones.

Para garantizar la seguridad de los Datos de Carácter Personal, el personal que pertenece a empresas proveedoras deberá observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:

El personal sólo podrá crear ficheros que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

No se albergarán datos de carácter personal en las unidades locales de disco de los puestos PC de usuario.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable y con respeto a la presente política.

Los soportes informáticos que contengan datos de carácter personal deberán ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

Intercambio de información

La distribución de información ya sea en formato digital o impreso, se llevará a cabo utilizando los recursos establecidos en el contrato de provisión de servicios o suministros o con adhesión a la presente política, exclusivamente con el fin de facilitar las funciones asociadas a dicho contrato. Zelestra se reserva el derecho de implementar medidas de control, registro y auditoría sobre estos recursos de difusión, en función de los riesgos identificados y el alcance del servicio u operaciones.

Con respecto al intercambio de información dentro del marco del contrato de provisión de servicios, se considerarán actividades no autorizadas las siguientes:

- Encubrir o manipular la identidad de cualquier persona en ninguna circunstancia.
- Transmitir o recibir material protegido por derechos de autor infringiendo la Ley de Protección de Propiedad Intelectual.
- Transmitir o recibir cualquier tipo de material ofensivo, declaraciones discriminatorias u otro tipo de declaraciones o mensajes que puedan considerarse ofensivos o ilegales.
- Transmitir o recibir juegos y/o aplicaciones no relacionadas con el negocio.
- Participar en actividades en Internet, como grupos de noticias o juegos, que no estén directamente relacionadas con el servicio prestado.
- Llevar a cabo cualquier actividad en Internet u otros medios que pueda perjudicar la buena reputación de Zelestra.

Además, cualquier divulgación de información que contenga datos de carácter personal, ya sea en soportes informáticos, en papel o por correo electrónico, solo podrá ser realizada por personal autorizado y con el debido permiso, cumpliendo con las leyes aplicables.

Uso apropiado de los recursos

El proveedor se compromete a utilizar los recursos asignados para la prestación del servicio de acuerdo con las condiciones establecidas.

Los recursos puestos a disposición del personal externo por Zelestra, independientemente de su naturaleza (equipos informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplir con las obligaciones y los propósitos operativos establecidos en los acuerdos de prestación del servicio. Zelestra se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso adecuado de dichos recursos.

Cualquier archivo introducido en la red o en cualquier equipo conectado a ella, ya sea a través de medios automatizados, Internet, correo electrónico u otros medios, deberá cumplir con los requisitos establecidos en esta política, especialmente en lo referente a la propiedad intelectual, protección de datos personales y control de virus.

Al finalizar el contrato, todos los activos físicos deberán ser devueltos a Zelestra, y los activos de información deberán ser destruidos o devueltos sin demoras injustificadas.

Se prohíbe expresamente:

- El uso de los recursos proporcionados por Zelestra para actividades no relacionadas con el propósito del servicio.
- La conexión a la red de equipos y/o aplicaciones sin el conocimiento y aprobación de Zelestra.
- La introducción de contenidos obscenos, amenazantes, inmorales u ofensivos en los sistemas de información o la red de la compañía.
- La introducción intencional de cualquier tipo de malware, dispositivo lógico, dispositivo físico o cualquier otra secuencia de comandos que pueda causar o sea susceptible de causar alteraciones o daños en los recursos informáticos.
- Intentar obtener derechos o accesos distintos a los asignados explícitamente.
- Intentar distorsionar o alterar los registros de actividad ("log") de los sistemas de información.
- Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad utilizado en los procesos telemáticos.
- Poseer, desarrollar o ejecutar programas que puedan interferir en el trabajo de otros usuarios o dañar o alterar los recursos informáticos de la organización.
- Intentar destruir, alterar, inutilizar o dañar de cualquier otra manera los datos, programas o documentos electrónicos de responsabilidad de Zelestra.
- Instalar en cualquier sistema de Zelestra cualquier software que no haya sido previamente autorizado, ya sea licenciado o de libre distribución.

Responsabilidades del usuario

Los proveedores de servicios deberán asegurarse de que todo el personal que realiza labores para Zelestra cumpla con los siguientes principios básicos en su actividad:

- Cada persona con acceso a la información de Zelestra es responsable de las actividades realizadas con su identificador de usuario y de todo lo derivado de ello. Por lo tanto, es fundamental que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, asegurando que la contraseña asociada sea conocida únicamente por el propio usuario y no debe ser revelada a otros miembros del personal en ningún caso.
- Los usuarios no deben utilizar el identificador de usuario de otra persona, incluso si cuentan con la autorización del propietario.
- Los usuarios deben conocer y aplicar los requisitos establecidos en relación con la información manejada.

Cualquier persona con acceso a información responsabilidad de Zelestra deberá seguir las siguientes directivas relacionadas con la gestión de las contraseñas:

- Seleccionar contraseñas de calidad.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.

Cualquier persona con acceso a la información de Zelestra debe asegurarse de que los equipos estén protegidos cuando vayan a quedar desatendidos. Se deberá respetar al menos las siguientes medidas de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:

- Almacenar bajo llave los documentos en papel y los medios informáticos con información de Zelestra en un mobiliario seguro cuando no estén en uso, especialmente fuera del horario de trabajo.
- No dejar desatendidos los equipos asignados a funciones críticas de Zelestra y bloquear su acceso cuando sea necesario y el equipo no esté siendo atendido.
- Proteger los puntos de recepción y envío de información (correo postal, máquinas de escaneo y fax) y los equipos de duplicación (fotocopiadoras, fax y escáneres) siempre que se utilice información de Zelestra. La reproducción o envío de información utilizando estos dispositivos será responsabilidad del usuario.
- Retirar de forma inmediata cualquier información confidencial una vez que se haya impreso.

Equipos de usuario

Los proveedores de servicios deben asegurarse de que todo el equipo informático utilizado por los usuarios para acceder a la información de Zelestra cumple con las siguientes medidas:

- Cuando un puesto de trabajo quede desatendido durante un breve período de tiempo, el sistema deberá activar su bloqueo automáticamente.
- Ningún equipo de usuario debe contar con herramientas que puedan infringir el sistema de seguridad y las autorizaciones establecidas en los sistemas de la organización.
- Los equipos de usuario deben mantenerse de acuerdo con las especificaciones del fabricante.
- Todos los equipos de usuario deben estar debidamente protegidos contra el malware, siguiendo estas directrices:
    - Se debe instalar y utilizar software antivirus para reducir el riesgo operacional asociado con virus y otro software malicioso.
    - Se deben mantener actualizados con las últimas actualizaciones de seguridad disponibles.
    - El software antivirus debe estar siempre habilitado y debidamente actualizado.

Se debe prestar especial atención a la seguridad de todos los dispositivos móviles utilizados por los usuarios que contengan información de Zelestra o que permitan acceder a ella de alguna manera. Esto se logra mediante las siguientes medidas:

- Verificar que los dispositivos móviles no contengan más información de Zelestra de la estrictamente necesaria.
- Aplicar controles de acceso a la información almacenada en dichos dispositivos.
- Minimizar el acceso a la información en presencia de personas no autorizadas al servicio proporcionado.
- Tomar precauciones adicionales fuera de las instalaciones de Zelestra para evitar que terceros accedan accidentalmente a la información confidencial.

Gestión de equipamiento

En caso de que Zelestra suministre equipos u otros activos de información, es importante que los proveedores de servicios se aseguren de una gestión óptima de estos, y de aquellos utilizados para la prestación de servicios. Con este objetivo, es fundamental cumplir con las siguientes medidas:

- El proveedor debe mantener una lista actualizada de los equipos y los usuarios asociados a dichos activos, o los responsables designados en caso de que los activos no sean de uso exclusivo de una persona. Esta lista estará a disposición de Zelestra en cualquier momento que sea requerida.
- Si un proveedor desea retirar un equipo de la lista de activos de Zelestra, deberá devolver dicho activo para que pueda gestionarse adecuadamente su baja.

- En caso de que un proveedor finalice la prestación del servicio, deberá devolver todos los equipos proporcionados de acuerdo con los contratos de prestación de servicios correspondientes. Únicamente en el caso de los activos de información, el proveedor podrá llevar a cabo su eliminación segura, siempre y cuando notifique a Zelestra sobre dicha eliminación.

Controles de acceso a las redes y servicios asociados

Los criterios de acceso se ajustan a las siguientes directrices:

- Los usuarios tendrán exclusivamente acceso a las redes, servicios de red y activos de información autorizados en función de sus responsabilidades laborales. Consecuentemente, la empresa proveedora deberá informar a Zelestra en caso de baja de cualquier empleado para que se eliminen sus accesos.
- Es imprescindible obtener una autorización previa para acceder a redes y servicios.
- La seguridad exige que el acceso a redes y servicios de red se someta a una supervisión constante.

En caso de crearse cuentas de dominio de Zelestra asociadas a proveedores que ofrecen sus servicios dentro de la organización, éstas serán conservadas durante el tiempo necesario para garantizar la trazabilidad de los registros de actividad asociados a dichas cuentas.

Es responsabilidad de ambas partes garantizar la seguridad de la información, lo que implica la obligación de informar de inmediato cualquier incidencia o anomalía relacionada con la seguridad de los sistemas de información/activos en operación que se pueda detectar, como virus, deterioro de medios, accesos no autorizados de terceros, entre otros. Estas comunicaciones deben realizarse a través de los canales de comunicación establecidos.

Es crucial proteger los flujos de información entre los sistemas de información de Zelestra y los del proveedor, y es obligatorio informar de cualquier incidente de seguridad que pueda afectar al servicio proporcionado.

Incumplimiento normativo

En el caso de que se identifique una violación a lo establecido en la presente política, Zelestra se reserva el derecho de tomar las medidas que considere apropiadas en relación con la tercera parte. Estas medidas pueden incluir la resolución de los contratos vigentes con dicho proveedor.

Actualización de los requisitos de seguridad

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, Zelestra se reserva el derecho a modificar estos requisitos cuando sea necesario. Los cambios realizados serán divulgados a todas las terceras partes a las que les aplique utilizando los medios que se consideren pertinentes.

Es responsabilidad de cada empresa garantizar la lectura y conocimiento de los requisitos más recientes de Zelestra por parte de su personal.

Sistema de seguimiento

La aprobación de la Política de seguridad de la información para terceras partes es responsabilidad del área de Digitalización y Ciberseguridad, mediante su Chief Digital Officer quien es miembro y parte del Comité de Dirección de la compañía, el cual, bien directamente o bien a través del Comité de Seguridad de la Información, supervisará la misma, velará por su cumplimiento y revisará periódicamente su continua idoneidad.

La Sociedad establecerá un sistema de seguimiento interno que permita la correcta implementación de la Política en todos los niveles organizativos.

Comunicación y participación de los grupos de interés

Esta Política es comunicada y entendida en el ámbito de la organización y está disponible a través de los canales de información y comunicación que la Compañía pone a disposición de todos sus grupos de interés.

La Política está disponible públicamente en el sitio web de Zelestra.

Con el fin de facilitar que cualquier persona pueda comunicar de manera confidencial y/o anónima cualquier incumplimiento de los principios descritos en la presente Política, se facilita el Canal Ético de Zelestra (https://zelestra.integrityline.com/) que garantiza la independencia, la imparcialidad y la ausencia de conflictos de intereses durante todo el proceso de recepción, tramitación y resolución de estas.

Alcance

Esta política se aplica a todas las actividades desarrolladas por personal que presta servicios o suministros a cualquiera de las sociedades del grupo Zelestra pero que pertenece a otras empresas, vinculadas a través del correspondiente contrato de provisión de servicios o suministros, independientemente del tipo de servicio proporcionado, y que en el desarrollo de sus funciones puedan tener acceso a información, sistemas de información, activos en operación o recursos de Zelestra.