POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

R.1

POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de la Fundación Pascual Tomás, fundación de carácter cultural y educativa y benéfico-docente, ha establecido e implantado un Sistema de Gestión de Seguridad de la Información basándose en los requisitos de la norma UNE-ISO/IEC 27001 respecto a las actividades de formación profesional para el empleo dirigida a las trabajadoras y trabajadores para su aprendizaje a lo largo de la vida laboral en las instalaciones de la Plaza de José María Orense en Valencia.

Las directrices en las que nos basamos para el cumplimiento de los requisitos de nuestros clientes y usuarios/as son:

- Comunicación eficaz dentro de la organización a todos los niveles de responsabilidad y participación en materia de seguridad de la información.
- Cumplir con los requisitos aplicables a la seguridad de la información.
- Mejora continua del sistema de gestión de seguridad de la información.
- Identificar, evaluar y minimizar, cuando sea posible, los riesgos a los que se expone la información de la Fundación y la de los clientes.
- Preservar en todo momento la disponibilidad, integridad y confidencialidad de la información como medio para garantizar el correcto desempeño de los servicios que prestamos a nuestros clientes frente a las potenciales amenazas que pudieran acontecer.
- Identificar y proteger los activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, manuales, estrategia, gestión, y otros conceptos.
- Obtener el más alto nivel de garantía en el tratamiento y custodia de la información que utilizamos y procesamos. A lo largo de su ciclo de vida, toda la información será protegida en la manera que la Fundación considere razonable y apropiada, según sea su nivel de sensibilidad, valor y criticidad.

Con objeto de cumplir nuestra Política, la Dirección ha documentado el sistema de gestión de seguridad de la información, y proporciona todos los recursos necesarios para el óptimo cumplimiento del mismo.

POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Se han diseñado unas políticas que deben ser llevadas a cabo a la hora de acceder a la información de la organización y que responden a la siguiente clasificación:

1. POLITICA DE DISPOSITIVOS MÓVILES

La Fundación proveerá las condiciones para el uso de los dispositivos móviles (teléfonos y tablets, entre otros) de la Fundación. Así mismo, velará porque los trabajadores/as y clientes hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

1.1 Medidas de seguridad para uso de dispositivos móviles

- Los usuarios deben evitar usar los dispositivos móviles de la fundación en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles notifique una actualización disponible, aceptar y aplicar la nueva versión.

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth o infrarrojos en los dispositivos móviles asignados.
- Los usuarios deben evitar conectar los dispositivos móviles asignados por puerto USB a cualquier ordenador público, de hoteles o cafés internet, entre otros.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles asignados.
- Los usuarios no deben hacer un uso personal del equipo.
- Los usuarios deben proteger el acceso a su dispositivo móvil mediante contraseña.
- Los dispositivos móviles se apagarán fuera de la jornada laboral a no ser que haya orden contraria por parte de Dirección.

1.2 Uso de dispositivos móviles personales

- Durante el horario de trabajo no se pueden hacer fotografías ni grabaciones (video o audio) en el interior de las instalaciones de la Fundación Pascual Tomás.
- Los alumnos no pueden hacer uso del móvil personal dentro de las instalaciones de la Fundación Pascual Tomás.

2. POLITICA DE TELETRABAJO (no hay teletrabajo, solo para acceso remoto a intranet)

La Fundación establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Fundación; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.

2.1 Medidas de seguridad para teletrabajo

1. Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Fundación y deben acatar las condiciones de uso establecidas para dichas conexiones.
2. Los usuarios únicamente deben establecer conexiones remotas en ordenadores previamente identificados y, bajo ninguna circunstancia, en ordenadores públicos, de hoteles o cafés internet, entre otros.
3. Los usuarios deben bloquear sus equipos de trabajo en el momento de abandonar su puesto de trabajo.
4. Los usuarios no deben dejar encendidos los equipos de trabajo u otros recursos tecnológicos en horas no laborables.
5. Los ordenadores portátiles, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
6. Los ordenadores deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
7. Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
8. En caso de pérdida o robo de un equipo portátil, se debe informar de forma inmediata al responsable del SGSI para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
9. Los usuarios deben asegurar que sus mesas de trabajo se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

10. Cuando se presente un fallo o problema de hardware o software en un equipo de trabajo u otro recurso tecnológico propiedad de la Fundación, el usuario debe informar al responsable del SGSI donde se atenderá o derivará con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
11. La instalación, reparación o retiro de cualquier componente de hardware o software de los equipos de trabajo, dispositivos móviles y demás recursos tecnológicos de la Fundación, solo puede ser realizado por el responsable del SGSI, o personal de terceras partes autorizado por dirección.
12. Ver punto 3.5. Control de acceso remoto.

3. POLITICA DE CONTROL DE ACCESO

3.1 Del acceso a áreas críticas.

El acceso de personal se llevará a cabo de acuerdo a las normas y procedimientos establecidos por la Fundación.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

El acceso al CPD o centros de cableado está restringido al personal encargado del mantenimiento de los sistemas, en caso de visitas externas se realizan las mismas siempre escoltadas por un empleado del departamento de sistemas. El acceso general al CPD está restringido, cerrándose con llave y armando los sistemas de alarma disponibles.

El responsable de SGSI debe registrar el ingreso de los visitantes al CPD y a los centros de cableado que están bajo su custodia, en un registro ubicado en la entrada de estos lugares de forma visible.

3.2 De áreas seguras.

La Fundación proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Las entradas y salidas de personal, externo a la estructura, a las instalaciones de la Fundación deben ser registrados; por consiguiente, los trabajadores y personal ajeno (servicios, visitas, profesores, alumnos, etc.) deben cumplir completamente con los controles físicos implantados.

Los trabajadores de la Fundación y personal ajeno (servicios, visitas, profesores, alumnos, etc.) no deben intentar entrar a áreas a las cuales no tengan autorización.

3.3 Del control de acceso al equipo informático

Todos y cada uno de los equipos son asignados a un usuario, por lo que es de su competencia hacer buen uso de los mismos.

Cada trabajador se encargará de llevar a cabo las siguientes prácticas de Seguridad recomendadas en su equipo:

- Iniciar sesión como usuario del dominio de la organización y regirse por las normas en cuanto a política de contraseñas de la organización.
- Apagar el ordenador fuera del horario de trabajo, así como evitar el uso del mismo por terceras personas.
- Proteger el escritorio del mismo durante las ausencias del puesto de trabajo en horario de oficina, mediante el bloqueo del PC. Los equipos se configuran con protección por contraseña que se activa tras un período de inactividad.
- No revelar las contraseñas personales a nadie, no registrarlas en ningún soporte que no garantice la correcta protección de las mismas como por ejemplo, soporte papel.
- Emplear el correo proporcionado por la organización de una manera responsable y siempre únicamente en el ámbito profesional, evitándose hacer uso de ella en para el ámbito privado.
- No emplear recursos productivos facilitados por la Fundación para usos no pertinentes.
- Comunicar cualquier incidencia de Seguridad (posible virus, comportamientos sospechosos...) al Responsable del SGSI.
- El acceso a información corporativa se realizará a través de la red de datos corporativa.
- El acceso a datos corporativos también se realizará mediante la Intranet, cuyo acceso estará limitado a los usuarios que deban usarla mediante autenticación por nombre de usuario y contraseña.

3.4 De control soporte en papel.

Es responsabilidad de todo empleado no dejar abandonada información confidencial en la impresora, fax o dispositivos similares, así como dejarla desatendida en el puesto de trabajo.

La documentación en papel se archivará por tipo de documentación en las oficinas de administración o el archivo.

3.5 De control de acceso remoto.

La organización dispone de una conexión remota a su red para usuarios fuera de su puesto de trabajo.

Los permisos serán los mismos que desde su puesto de trabajo local y la conexión remota se realiza de forma cifrada para autenticarse. El usuario remoto se compromete a adoptar las medidas de Seguridad en su equipo para garantizar que el acceso a los datos se realiza de manera responsable.

El usuario de estos servicios deberá sujetarse a lo expuesto anteriormente sobre acceso local al equipo y en concreto:

Deberán disponer de antivirus actualizado y en funcionamiento, aplicarse las actualizaciones y parches de seguridad más reciente y no deberá recordar la contraseña de VPN en el sistema.

3.6 Del acceso a Internet.

Los accesos a Internet a través de los navegadores deben sujetarse a las normas éticas y es responsabilidad de cada usuario realizar un uso lícito de los medios de que le provee la organización para el correcto desempeño de su trabajo.

El acceso Web a la Intranet de la Organización se realizará desde cualquier puesto de trabajo y es protegido mediante el control de accesos.

Toda la programación involucrada en la tecnología Web deberá cumplir unos requisitos de calidad y de seguridad.

El material que aparezca en la página web deberá ser aprobado por Dirección, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

Está prohibido representar a la organización en foros, listas de correos, etc. sin la autorización expresa de la Dirección.

3.7 De utilización de los recursos de la red.

Todos los empleados que utilicen los Sistemas de Información de la Organización deben firmar la aceptación de esta política de Seguridad. Al firmar esta política, el empleado acepta comprender y comprometerse al cumplimiento de las políticas y procedimientos de la organización relativas al uso de los Sistemas de Información, incluyendo las normas de la política.

El uso del correo electrónico para comunicaciones corporativas estará limitado a las cuentas de la organización y deberá cumplir con el propósito del desempeño del trabajador.

La cesión de datos a través de este medio deberá estar autorizada para la finalidad exclusiva para la cual sea necesario. Está prohibido copiar, sin justificación o autorización, información propia de la organización o software. Aquellos responsables de reenvío de información a terceros sin autorización estarán sujetos a la aplicación de medidas disciplinarias. Incluido en este apartado está la prohibición de enviar cartas o solicitudes, así como transmitir cualquier software no validado por la organización.

Se hará un uso responsable de otras cuentas personales para uso particular en la organización.

Será responsabilidad del usuario la apertura de mensajes de correo. Se aconseja no abrir correos electrónicos no solicitados, de remitentes desconocidos o sospechosos. Es responsabilidad igualmente del usuario el buen uso del correo electrónico, si bien se dispondrán las medidas técnicas por parte de la Fundación para evitar el spam de correo, las cuentas no autorizadas, etc. Debido a que las cuentas de correo electrónico corporativas son cedidas por la organización para uso profesional del empleado, el usuario deberá atenerse a las reglas establecidas para su uso por la organización.

Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.

4. POLITICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS

La Fundación velará porque la información, clasificada como confidencial o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio, con el propósito de proteger su confidencialidad e integridad.

5. POLITICA DE GESTIÓN DE CLAVES

Todos los empleados que necesitan acceso a algún Sistema de Información de la organización disponen de un Identificador ID de usuario único y una contraseña personal.

El usuario asociado a cada empleado está conforme a los privilegios que corresponden a sus funciones, responsabilidades y actividades.

Todos los usuarios son responsables de proteger sus identificadores de usuario y contraseñas.

Las contraseñas escogidas por los usuarios deben ser difíciles de adivinar y no deben contener información relacionada con su trabajo y su vida personal: Números de teléfono, nombre de familiares, direcciones, números personales (PIN, SIN, DNI…), lugares conocidos, etc.

Las contraseñas deben ser cambiadas con la periodicidad y cumplir las normas establecidas para cada sistema.

Las contraseñas no deben ser almacenadas en ficheros legibles, macros, PCs sin control de acceso o ningún otro lugar donde puedan ser accedidas por personas sin autorización.

Los administradores del sistema y personal técnico nunca solicitarán la contraseña a sus usuarios. La única excepción es la asignación inicial de la contraseña personal con el compromiso por parte del usuario de cambiarla inmediatamente en el primer acceso al sistema.

Si un usuario sospecha que su identificador y contraseña está siendo utilizado ilegalmente, es su responsabilidad avisar inmediatamente al Responsable del SGSI.

6. POLITICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

En la Fundación se realizan las siguientes normas de seguridad con respecto a este apartado:

- Se dispone de destructora de papel para la eliminación de documentación
- Los empleados tienen la obligación de no dejar desatendida documentación (especialmente si es confidencial) encima de las mesas. Toda información confidencial debe guardarse en los lugares habilitados al respecto y a ser posible bajo llave.
- Proteger el escritorio del ordenador durante las ausencias del puesto de trabajo en horario de oficina, mediante el bloqueo del PC. Los equipos se configuran con protección por contraseña que se activa a los 10 minutos de inactividad del equipo.

7. POLITICA DE INTERCAMBIO DE INFORMACIÓN

Solo se permite dicha cesión cuando esté regulada por un acuerdo entre ambas partes para el intercambio de dicha información y en el mismo se defina la finalidad exacta de dicha cesión, así como la caducidad de la misma y la garantía de supresión de la misma una vez cumplido el objetivo de la cesión.

Asimismo, queda regulada la cesión de información a terceras personas, quedando estrictamente prohibida la cesión de información sensible de la Organización fuera de los procedimientos establecidos, siendo necesaria la autorización de la Dirección para cualquier salida de información fuera de la Fundación.

8. POLÍTICA DE SOPORTES EXTRAIBLES

Se prohíbe expresamente la salida de soportes de información extraíble (dispositivos de almacenamiento USB, memorias flash, etc.) con datos confidenciales o restringidos de la Fundación sin el consentimiento expreso del Responsable del SGSI y con las medidas de seguridad adecuadas. Cuando se usen dichos dispositivos dentro de la Fundación los usuarios deben ser conscientes de ejecutarlos

solo en equipos con antivirus actualizados y conocer perfectamente el origen de dicho medio y que sea confiable.

Cualquier información que sea almacenada en un soporte de información extraíble deberá ser empleada exclusivamente para motivos de trabajo y la información deberá eliminarse de manera segura o guardarse bajo llave una vez deje de ser útil. Ver procedimiento de gestión de soportes.

9. POLITICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEDORES

Se firmará un acuerdo de confidencialidad con los proveedores que tengan acceso a información confidencial o restringida de la organización.

Cumplir los requisitos de la reglamentación en materia de LOPD.

10. POLITICA DE DESARROLLO SEGURO DE APLICACIONES Y SISTEMAS

La seguridad en los productos software se tratará como un conjunto de actividades a lo largo del ciclo de desarrollo, desde su misma concepción hasta la muerte del producto, que nace con la idealización del sistema, y se extiende sobre el diseño, la codificación y el fortalecimiento del mismo.

No se debe confundir la seguridad del sistema con las características de éste ni con los componentes de seguridad que se ven inmersos en la arquitectura del sistema, como la presencia de firewalls, o limitarla al cumplimiento de una normativa o certificación en particular.

La seguridad del producto es una propiedad dinámica que varía en el tiempo y que resulta crítica. Surge tras reconocer que existen atacantes, y que estos se encuentran siempre dispuestos a probar cada potencial camino de entrada para lograr el control del sistema, y por tanto nos fuerzan a pensar mecanismos de control para resistir estos ataques.

Diseño seguro:

1. Ningún componente es confiable hasta demostrar lo contrario.
2. Delinear mecanismos de autenticación difíciles de eludir.
   La autenticación es el proceso que nos permite acreditar la identidad del usuario y asignarle un identificador único. El desarrollo de métodos autenticación centralizados que cubran cada posible camino de ingreso es uno de los pilares en la construcción de aplicaciones seguras.
   Si se trata de páginas web, debemos pensar qué sitios requerirán el manejo de usuarios autenticados, y cuidar que terceros indebidos no se entrometan en el sistema desde URLs no protegidas. La utilización de múltiples factores de autenticación nos permitirá reforzar el sistema.
3. Autorizar, además de autenticar.
   La autorización es el proceso que designa si un usuario autenticado puede o no realizar una acción que cambia el estado del sistema. Los procesos de autorización sobre usuarios autenticados deben ser pensados desde el diseño y previenen contra sesiones que han caído en las manos equívocas.
4. Separar datos de instrucciones de control.
   Este punto es clave cuando se trabaja con código capaz de modificarse a sí mismo, o lenguajes que compilan dicho código en tiempo de ejecución -tales como JavaScript-, donde las mismas instrucciones se reciben como datos. Entonces, se vuelve de suma importancia sanear las entradas que recibe el sistema para evitar que atacantes puedan manipular el flujo de ejecución ingresando datos maliciosos.
5. Validar todos los datos explícitamente.

Las entradas al sistema deben evaluarse determinando qué se permitirá, y denegar todo aquello que no se corresponda. Debemos pensar que un atacante interpreta los datos como posibles lenguajes de programación, con la intención de manipular el estado del sistema. Por esto, se torna necesario inspeccionar estos datos de entrada, generando los procedimientos automáticos para llevarlos a formas canónicas bien conocidas.

Además, esta validación de entradas debe darse cercana al momento en que los datos son en efecto utilizados, puesto que el desfasaje entre la validación y la utilización brinda una ventana de oportunidad para la generación de ataques.

Para implementar esto, pueden diseñarse componentes comunes que centralicen validaciones tanto sintácticas –estructurales– como semánticas –de significado–, y sacar provecho de los tipos de datos presentes en el lenguaje de programación sobre el cual se está trabajando.

6. Utilizar criptografía correctamente.
   La comprensión de las nociones criptográficas que aplican al sistema en desarrollo es necesaria para poder entender qué elementos y qué característica de los mismos se busca proteger, contra qué formas de ataque, y consecuentemente, cuál es la mejor manera de lograr este objetivo.
7. Identificar datos sensibles y cómo se los debería gestionar.
   La definición de los datos cuya protección resulta fundamental para el funcionamiento del sistema es crítica, puesto que a partir de ella podremos comenzar a esbozar los procesos para el diseño de la seguridad desde el mismo comienzo del ciclo de desarrollo, y no como un añadido en las etapas de implementación o despliegue.
   La definición de los requerimientos de anonimidad y los metadatos que se manejan dará pie a la toma de decisiones en cuanto a los caminos que hacen a su protección.
8. Considerar siempre a los usuarios del sistema.
   La seguridad utilizable debe ser una de las metas a alcanzar cuando se plantean los objetivos de seguridad para el sistema. Es necesario mantener una comunicación con el usuario para otorgar cierto grado de transparencia sobre cómo opera el sistema. La configuración por defecto debe ser la configuración segura, siempre.
9. La integración de componentes cambia la superficie de ataque.
   Las aplicaciones actuales constituyen sistemas complejos con muchos componentes interactuando de manera simultánea. Cada vez que se realiza un cambio en el sistema, el panorama de seguridad cambia y debe ser reevaluado.
   Los componentes deben ser analizados de manera unitaria y en conjunto, teniendo en cuenta cómo se combinan, mantienen o reemplazan.
10. Considerar cambios futuros en objetos y actores.
    Desde el diseño, debemos considerar que las propiedades del sistema y sus usuarios cambian constantemente. Algunos factores a considerar son el crecimiento de la población de usuarios, cómo las migraciones afectan al sistema, o cómo afectarán vulnerabilidades futuras sobre componentes que se han desplegado a gran escala.
    Los procedimientos de actualización de manera segura deben de diseñarse con un horizonte a futuro de meses, años o incluso décadas.

La identificación y remediación temprana de problemas posee un costo inversamente proporcional al tiempo que el error permanece en el sistema.

La instauración de un ciclo de desarrollo seguro mediante la instrumentación de un modelo de diseño orientado a la seguridad que genere sinergia entre el área de seguridad y desarrollo, nos acerca un paso más hacia el despliegue de aplicaciones más robustas y mucho más rentables.

11. POLITICA DE DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO
  - Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
  - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
  - No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
  - No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
  - El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con LA EMPRESA

- DERECHOS DE LOS TITULARES DE LOS DATOS
  Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL
  Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

- CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)
  - UBICACIÓN DE LAS CÁMARAS: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.
  - UBICACIÓN DE MONITORES: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.
  - CONSERVACIÓN DE IMÁGENES: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.
  - DEBER DE INFORMACIÓN: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo.

- CONTROL LABORAL: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.
- DERECHO DE ACCESO A LAS IMÁGENES: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.
  No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

- IDENTIFICACIÓN
  - Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
  - Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
  - Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
  - Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
  - Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

- DEBER DE SALVAGUARDA. A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

  - ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la medida posible.
  - MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
  - CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
  - CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

- COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.

12. PROCESO DISCIPLINARIO

Los empleados que deliberadamente o por negligencia incumplan la Política de Seguridad de la información estarán sujetos a acciones disciplinarias.

Las acciones disciplinarias en respuesta a los incumplimientos de la Política de Seguridad de la Información son atribución de la Dirección de la Fundación.

Cualquier violación de las políticas y normas de seguridad será sancionada de acuerdo a los mecanismos habilitados por la legislación vigente.

Todas las acciones en las que se comprometa la seguridad de la información de la Fundación y que no estén previstas en esta política, deberán ser revisadas por Dirección y por el Responsable del SGSI para dictar una resolución sujetándose al criterio de la organización y la legislación prevista.

Todo empleado es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.

Todo usuario como propietario de la información que genere se responsabilizará de la misma y de su correcto almacenamiento.

Todo empleado es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.

Esta política de seguridad estará disponible para todo el personal involucrado en la relación con la Organización que maneje datos y recursos pertenecientes a la misma. Asimismo, en caso de realizarse cambios, esta política se actualizará en los repositorios habilitados por la Fundación y en su caso comunicado a todo el personal.

Con una periodicidad mínima anual se revisará esta política de Seguridad para adecuarla a los posibles cambios en la Organización.

La presente Política de Seguridad de la Información ha sido aprobada por la Dirección, con vigencia a partir de la fecha de su firma.

En Valencia, a 10 de diciembre de 2018

Dirección