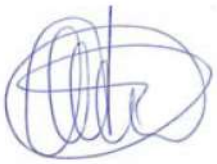
POLÍTICA DE SEGURIDAD Y ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	25/03/2020	Emisión inicial
01	09/04/2021	Actualización del formato

REVISADO Y APROBADO:

Firma:



Firma Juan Carlos Martínez Rodríguez
Fecha: 09/04/2021

Contenido

1. OBJETO

Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos empresariales y con la legislación y las normativas aplicables.

La Dirección de OPEMAT INGENIERÍA, S.L. manifiesta su apoyo y compromiso con la seguridad de la información a través de la publicación de la Política, en la que se establecen las líneas de actuación generales a seguir.

2. ALCANCE

Las Políticas de seguridad de la información se aplicarán a toda aquella información y procesos que la apoyan (sistemas y redes) cuya disponibilidad, integridad y confidencialidad pueden ser esenciales para mantener la competitividad, rentabilidad, cumplimiento de la legalidad e imagen comercial de OPEMAT INGENIERÍA, S.L.

3. POLÍTICA DE SEGURIDAD

3.1. Política de seguridad

La Política general de Seguridad establece los principios básicos, normas y requisitos aplicables a OPEMAT INGENIERÍA, S.L. y que se consideran esenciales en la preservación de la seguridad de la información.

La Política general de Seguridad de la Organización está definida dentro del documento Política Integrada del Sistema. Este documento ha sido aprobado por la Dirección y puesto a disposición de todos los empleados y de las partes externas relevantes.

De esta Política general derivan las diferentes Políticas de Seguridad de la Información, que contendrán los requisitos de la norma para este apartado. Éstas se comunicarán a los empleados dentro de los programas de concienciación, formación y educación en seguridad de la información.

3.2. Revisión de la política de seguridad

Con el fin de detectar su idoneidad, eficiencia y efectividad, la Política de Seguridad de la Información será revisada anualmente por el Comité de Gestión de SI de la empresa, compuesto por la Dirección y el Responsable del Sistema, o cada vez que se produzcan cambios en la organización que así lo requieran.

Mediante estas revisiones se tratará de dar respuesta a los cambios que se produzcan en los aspectos anteriores, con el objetivo de asegurar que dicha Política está actualizada y es realmente efectiva. Los puntos tratados y decisiones tomadas en esta revisión deberán ser consolidados en el Informe de Revisión por Dirección.

4. ORGANIZACIÓN INTERNA

4.1. Compromiso de la dirección

El cumplimiento de los objetivos y principios de aseguramiento de la Seguridad de la Información es un objetivo compartido por toda la organización y es responsabilidad directa de la Dirección de OPEMAT INGENIERÍA, S.L. La Política de Seguridad de la Información ha sido desarrollada bajo la supervisión de la Dirección, y cuenta con su total apoyo y compromiso.

La Dirección delega su representación en temas de seguridad al **Responsable de Gestión de Seguridad de la Información**, al cual le confiere autoridad y responsabilidad para asegurar la eficaz implantación del Sistema de Gestión de Seguridad de la Información, así como su adecuación a la evolución tecnológica, industrial y comercial de la Organización. Además, la Dirección participará activamente en las acciones de revisión y seguimiento del SG de seguridad de la información.

Si surgieran problemas o diferencias de opinión que no pudieran resolverse de acuerdo con las instrucciones de seguridad establecidas, éstos deberán ser sometidos a análisis del **Comité de Gestión de SI**.

4.2. Comité de gestión para la seguridad de la información

La Dirección muestra su apoyo de cara a la Seguridad de la Información a través de la definición, aprobación y comunicación de la Política de Seguridad, y expresa su compromiso documentalmente a lo largo de los procedimientos y registros del sistema; además pone a disposición de los miembros de la organización los recursos y medios necesarios para la implantación y operación del SG.

Por último la dirección establece que el Comité de Gestión de Seguridad de la Información estará formado por la Dirección y el Responsable del Sistema.

4.3. Asignación de responsabilidades

La asignación de responsabilidades en materia de seguridad se realizará a través de los siguientes mecanismos:

- Responsabilidades definidas en los perfiles de puesto de trabajo
- Responsabilidades definidas en cada uno de los procedimientos del SG
- Identificación del propietario o responsable de los activos realizada en el inventario de activos o en las fichas de personal

4.4. Segregación de tareas

Las funciones y áreas de responsabilidad deben segregarse en la medida de lo posible para evitar modificaciones no autorizadas o usos indebidos, si bien por las características de la organización, es

difícil de implementar; dirección se encarga de la supervisión de las mismas para la consecución de este control.

4.5. Proceso de autorización de recursos para el tratamiento de la información

Cuando sea necesario instalar nuevos recursos para el procesamiento de información se seguirá el siguiente procedimiento:

- Se comunicará la necesidad del nuevo recurso junto con las características del mismo al Responsable del Sistema
- El Responsable del Sistema analizará la petición junto con las posibles alternativas técnicas. Si considera oportuna el nuevo recurso trasladará la petición a la Dirección quien deberá autorizar su implantación

4.6. Acuerdos de confidencialidad

OPEMAT INGENIERÍA, S.L. se asegurará de que el personal de la organización es consciente de sus responsabilidades de confidencialidad o no revelación, mediante la firma por todos los empleados en el momento de su incorporación a la organización, de un **acuerdo de confidencialidad** que refleje las necesidades de la empresa para la protección de la información.

Los acuerdos de confidencialidad serán revisados anualmente, o cuando las necesidades de la organización así lo requieran.

En el caso de convenios con terceros, se seguirá el procedimiento establecido en el **punto 5. Terceros**, del presente documento.

4.7. Asesoramiento especializado

En aquellos casos en que se considere necesario por limitaciones de la Organización a la hora de dar respuesta o implantar determinados controles, se podrá solicitar el asesoramiento de un externo en Seguridad de la Información, siendo el Responsable del Sistema el interlocutor interno responsable de la coordinación con dicho asesor.

4.8. Contacto con las autoridades

De cara a garantizar el cumplimiento de las Políticas y normas de seguridad establecidas por la Organización, así como garantizar el cumplimiento de la legislación vigente, la organización establece las siguientes pautas de actuación:

- Está a disposición de todos los empleados un listado con los datos de contacto con los servicios de emergencia (salud, bomberos, policía, etc.).

- Todos los incidentes en materia de seguridad deberán ser registrados acorde a lo establecido en la Política de Gestión de Incidentes en materia de Seguridad de la Información.

- Cuando los incidentes remitan seria gravedad, el Responsable del Sistema o la Dirección podrán solicitar asesoramiento o tramitar las denuncias correspondientes ante las siguientes autoridades:

    - Guardia Civil: cuándo se identifique un problema de seguridad en la red, se localice un contenido ilícito o se crea haber detectado u observado una conducta delictiva. La dirección de contacto a través de internet es la siguiente: https://www.gdt.guardiacivil.es/

    - Agencia Española de protección de datos: en caso con incidentes o incumplimientos de los derechos de protección de datos se podrá contactar con la Agencia de Protección de Datos en las siguiente dirección: https://www.aepd.es/

    - CCN-CERT: cuándo se necesite información o asesoramiento sobre incidentes de seguridad de la información podrá recurrirse al Centro Criptológico Nacional, en el que se comparten objetivos, ideas e información sobre seguridad de forma global. https://www.ccn-cert.cni.es/

    - BSA: ante problemas o incidentes relacionado con la piratería de software podrá consultarse o contactar con Business Software Aliance en las siguiente web: http://www.bsa.org

4.9. Contacto con grupos de especial interés

Con el objetivo de mejorar el conocimiento de las mejores prácticas de seguridad de la información, mantenerse al día sobre los cambios en la legislación aplicable, recibir advertencias tempranas sobre ataques y/o vulnerabilidades de seguridad, compartir información sobre tecnologías, productos, etc., la organización establece las siguientes actuaciones:

- Revisión periódica de los posibles cambios en la legislación aplicable (LOPD,…..) https://www.aepd.es/

- Consulta periódica de foros especializados en seguridad, que permitan mantenerse al día en temas de vulnerabilidades técnicas, virus y cualquier otro aspecto que pueda comprometer la seguridad de la información, como ejemplo:

    - https://www.mcafee.com/es-es/index.html

    - http://www.eset.es/centro-de-alertas/consejos-seguridad

- Subscripción a revistas especializadas, webpapers, RSS, etc.

- Participación en eventos, cursos, conferencias, coloquios, etc., relacionados con temas de especial interés.

La Dirección de OPEMAT INGENIERÍA, S.L. considerará el interés de pertenecer o entrar en contacto con grupos de interés especial, asociaciones profesionales, operadores de telecomunicaciones, etc. que le permita obtener su asesoramiento y adoptar rápidamente las acciones más adecuadas en caso de incidencias de seguridad.

4.10. Seguridad de la información en la gestión de proyectos

Este punto se aplica a todos los proyectos de la organización en general, ya que está aplicado a todo el Sistema de Gestión, y no se especifica a proyectos concretos.

4.11. Revisión independiente de la seguridad

En cumplimiento de la realización de auditorías independientes de seguridad de la información, OPEMAT INGENIERÍA, S.L. seguirá lo establecido en el procedimiento de Auditoría Interna. En dicho procedimiento se establecerá la periodicidad de realización de las auditorías (plan de auditorías) y las características a cumplir para garantizar la independencia de las auditorías realizadas.

5. TERCEROS

El objetivo principal de este punto, es el de asegurar la protección de los activos con los que cuenta la organización que son accesibles a terceros.

5.1 Política de si en las relaciones con proveedores

A la hora de identificar los riesgos para la seguridad relacionados con terceros, será necesario dar respuesta a las siguientes cuestiones:

- Tipo de acceso que se dará al tercero (acceso físico, lógico, recursos a los que accede, tipo de información a la que tiene acceso, etc.)
  En cuanto a acceso lógico, se tienen en cuenta los terceros que tienen acceso a la información, como pueden ser proveedores de servicios informáticos o gestorías.
- Motivos del acceso. Los terceros que trabajan para la organización de forma temporal pueden comprometer la seguridad de la información. Es necesario identificar qué medidas de control se necesitan para administrar el acceso de estos terceros. Entre los terceros que tienen acceso a las instalaciones de la Organización se encuentran, entre otros:
  - Servicio de limpieza
  - Servicio de mantenimiento de extintores
  - Consultores externos
  - Servicios de mantenimiento de suministros (luz, agua, gas, etc.)

Como norma general, en el caso de acceso de terceros se tomarán las siguientes medidas:

- Para aquellos terceros que tengan acceso a las instalaciones sin ningún tipo de supervisión por parte del personal de la Organización, o terceros que accedan a la información de la empresa, se establecerán contratos o acuerdos de confidencialidad en los que se reflejen las compromisos y responsabilidades asumidos por el tercero, de cara a garantizar la seguridad de la información (véase apartado 0 5.2. Requisitos de seguridad en contratos con terceros).
- Cuando los terceros tengan acceso controlado a las instalaciones, es decir, estén acompañados en todo momento por algún miembro de la Organización, no será necesario establecer ningún tipo de contrato o acuerdo.
- Salvo excepciones autorizadas por la Dirección de la Organización, los terceros nunca tendrán llaves ni claves de los sistemas de alarma o de control de acceso.

5.2. Requisitos de seguridad en contratos con terceros

Una vez identificados los riesgos relacionados con terceros, se establecerán las medidas de control que se implantarán para su administración. Así, el procedimiento a seguir a la hora de permitir un acceso a un tercero a las instalaciones:

1. Identificación de los riesgos relacionados a través de la lista descrita en la sección ¡Error! No se encuentra el origen de la referencia. Identificación de riesgos derivados del acceso de terceros.
2. Elaboración de los convenios de seguridad y confidencialidad a firmar por el tercero, en función de la identificación de riesgos anterior. Dichos convenios deberán incluir:
    - Informar sobre la Política General sobre Seguridad de la Información
    - Descripción de los servicios a los que tendrá acceso
    - Responsabilidades en materia de legislación (protección de datos personales, derechos de propiedad intelectual…)
    - Derecho de la Organización para controlar y suspender en su caso la actividad del usuario
    - Procedimientos y controles de seguridad implantados y de obligatorio cumplimiento

5.3. Cadena de suministro de ti y de las comunicaciones

Deberán tenerse en cuenta requisitos de seguridad de la información no solamente a nuestros proveedores sino también, a toda la cadena de suministro. Es decir, los riesgos para la seguridad de la información también están afectados por lo que nuestros proveedores subcontraten.

Se tendrán en cuenta dos principios para sostener una cadena de suministro con garantías:

- Elegir proveedores de confianza
- Exigir a los proveedores un control de seguridad a sus propios proveedores, en caso de que los tengan.

Actualmente, los proveedores con los que cuenta la Organización no subcontratan los servicios que le ofrecen a la misma, por lo que no ha sido necesario establecer controles; si bien se dejan especificados a continuación de cara a futuro.

Los controles que podemos aplicar a la cadena de suministro son:

- Establecer los criterios de seguridad para cada servicio, producto o tecnología de comunicación a subcontratar. La evaluación de riesgos enfocada a un servicio o producto en concreto, nos puede ayudar a establecer los criterios a la hora de subcontratar este servicio y determinar qué características o nivel de seguridad requiere a la hora de elegir al contratista.
- Establecer clausulas para el subcontratista en cuanto a que apliquen requisitos de seguridad a sus proveedores y a toda la cadena de suministro.
- Detallar que partes de los productos o servicios subcontratados a su vez requieren de otros proveedores externos y que requisitos y controles de seguridad se van a aplicar para garantizar la seguridad de la información
- Establecer procesos para comprobar que los productos o servicios suministrados cumplen con los requisitos establecidos para la seguridad de la información al menos para los productos y servicios que determinemos como fundamentales y que son adquiridos fuera de la organización.
- Exigir la trazabilidad de componentes críticos
- Establecer un proceso para comunicarnos con nuestros proveedores y la cadena de suministro

POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	25/03/2020	Emisión inicial
01	09/04/2021	Actualización del formato

REVISADO Y APROBADO:

Firma:

Firma Juan Carlos Martínez Rodríguez
Fecha: 09/04/2021

Contenido

1. OBJETO

Establecer los controles necesarios para que la realización de las actividades cotidianas de la organización garantice el cumplimiento de los objetivos de seguridad física y ambiental establecidos por la norma ISO 27001.

2. ALCANCE

La Política de seguridad física y ambiental será de aplicación a todos los miembros de la Organización para el uso correcto y seguro de los recursos e instalaciones de la misma.

3. ÁREAS SEGURAS

3.1. Objetivo

Evitar el acceso físico no autorizado, daño e intromisiones en las instalaciones y a la información de la Organización.

Los medios de procesamiento de información crítica o confidencial deberán ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deberán estar físicamente protegidos del acceso no autorizado, daño e interferencia.

3.2. Perímetro de seguridad física

Las instalaciones de OPEMAT INGENIERÍA, S.L. constan de un único local, ubicado en la primera planta de una nave industrial. El acceso a las instalaciones se realiza a través de la entrada principal a la nave. El acceso a las oficinas de la empresa está controlado por el personal técnico.

En cuanto a los perímetros de seguridad existente se puede destacar que la puerta de acceso se encuentra siempre cerrada y para acceder es necesario llamar para que abran desde el interior.

3.3. Controles físicos de entrada

Los controles físicos de entrada establecidos para los diferentes puntos de acceso a las instalaciones son los siguientes:

- El acceso por la puerta principal está controlado por un avisador electrónico.
- El acceso por la puerta de la propia oficina está controlado por el personal técnico.
- Los visitantes que acudan a las oficinas de OPEMAT INGENIERÍA, S.L. (clientes, proveedores, servicios de transporte o paquetería, servicios de mantenimiento, cartero, etc.), estarán siempre acompañados por un empleado y no se permitirá el acceso, salvo autorización

expresa de la Dirección, a ningún empleado ni visitante fuera del horario laboral o sin que alguien de la Organización esté presente.

3.4. Aseguramiento de oficinas, despachos e instalaciones

Además de las medidas de seguridad ya indicadas en los puntos anteriores se establecen las siguientes medidas de seguridad en las instalaciones:

- Las instalaciones constan de los extintores reglamentarios en correcto estado de revisión.
- La información de uso exclusivo de la organización (listados telefónicos, esquemas de red, documentos de uso interno, etc.) no estarán expuestos al alcance de terceros.
- En las oficinas y despachos habrá armarios provistos con llave para almacenar la información confidencial.

3.5. Protección contra amenazas externas e internas

El objetivo de las instrucciones recogidas en el presente apartado es asignar y aplicar protección física contra amenazas internas y externas: fuego, inundaciones, explosión, etc. En este sentido se establecen las siguientes medidas:

1. El Responsable del Sistema elaborará y revisará los **Planes de Continuidad** de la empresa. Esta revisión se realizará como mínimo de forma anual, o cuando se hayan producido incidentes o contingencias de seguridad física que así lo aconsejen: incendios, inundaciones, etc.
2. El Responsable del Sistema comunicará los **Planes de Continuidad** de la empresa a todos los empleados y partes interesadas.
3. No se permite el almacenamiento de materiales peligrosos o combustibles cerca de las áreas seguras. Los suministros a granel como por ejemplo los de papelería no deberán almacenarse en las áreas seguras.
4. Para daños provocados por incendios, se dispone de los extintores reglamentarios para su uso.
5. Cuando existan equipos o medios de reemplazo o respaldo, éstos deberán ubicarse a una distancia prudencialmente segura, para evitar que dichos equipos puedan ser dañados por el mismo desastre que afecte a los equipos que estén en producción.
6. El Responsable del Sistema deberá verificar que los sistemas de seguridad (extintores) son revisados con la periodicidad establecida.

3.6. Trabajo en áreas seguras

En OPEMAT INGENIERÍA, S.L. no se han definido áreas seguras como tal, aunque si se han establecido determinados equipos que merecen especial protección.

Los equipos sensibles, como el servidor, estarán bajo llave. Se establecen las siguientes normas para el trabajo en las inmediaciones del servidor:

- El lugar donde se ubica el servidor deberá estar cerrado con llave. El acceso a la llave únicamente lo tendrá la Dirección y el Responsable del Sistema.
- El Responsable del Sistema deberá supervisar y controlar la temperatura del servidor y para evitar daños producidos por las elevadas temperaturas. Este control deberá intensificarse en los meses de verano.
- No se permite almacenar material combustible o peligroso en la misma sala.
- No se permite almacenar o apoyar líquidos, bebidas, elementos magnéticos o cualquier otro material que pueda suponer o incrementar los riesgos de seguridad sobre el armario del servidor (incendio, cortocircuito, avería, etc.).
- Para acceder o manipular el servidor será necesario solicitar la llave al o al Responsable del Sistema, quiénes tomarán la decisión de permitir o denegar dicho acceso en función de las capacidades técnicas del solicitante.

3.7. Áreas de acceso público y de carga y descarga

La única zona de acceso público o carga y descarga es la recepción. La zona de acceso está controlada por el personal responsable de atención al público.

- Todos los terceros que accedan estarán acompañados y controlados por personal de la empresa.
- Los materiales o equipos que se recojan en esta área, serán reubicados y clasificados de acuerdo a las normas y procedimientos de la organización, garantizando las medidas de seguridad establecidas para las áreas seguras.

4. SEGURIDAD DE LOS EQUIPOS

4.1. Objetivo

El objetivo de las instrucciones aquí contenidas es evitar la pérdida, daño o robo de los activos y la consecuente interrupción de las actividades de la Organización.

Es necesario proteger los equipos contra las amenazas físicas y ambientales, incluidos aquellos utilizados fuera de las instalaciones de la Organización, para reducir el riesgo de acceso no autorizado a la información en ellos contenida, y evitar su pérdida, daño o robo. Se cuenta con un Listado de Equipos para un mejor control de los mimos.

4.2. Ubicación y protección

Es necesario situar los equipos con el objetivo de reducir los riesgos de amenazas del entorno.

Se tendrán en cuenta las siguientes consideraciones por parte de los empleados a la hora de situar y proteger el equipamiento:

- Los puestos de los trabajadores contarán con una orientación que dificulte que ninguna persona no autorizada pueda observar los procesos de información durante su uso.
- Los equipos deberán estar elevados del suelo, con una disposición que evite los riesgos ocasionados por inundaciones o fugas de agua, así como los posibles daños ocasionados por caídas o golpes.

  Todos los equipos de comunicaciones (por voz y datos) están situados también de forma que se evite su daño o destrucción, con una elevación suficiente y de forma que no se puedan producir caídas o golpes.
- En cuanto a la protección contra amenazas tales como robo, incendio, etc., se tendrán en cuenta todas las descritas en el apartado ¡Error! No se encuentra el origen de la referencia. del presente documento.
- No está permitido comer y/o beber junto a los equipos.
- En la empresa se observarán las normas de seguridad y sanidad exigibles en cada momento.

4.3. Suministro eléctrico

Para garantizar la protección del servidor contra fallos en el suministro eléctrico u otras anomalías eléctricas, éste se encontrará conectado a un SAI.

Dado que el servidor de la oficina es el equipo más crítico, si se prevé que el corte de corriente supere la autonomía del SAI, el Responsable del Sistema o la Dirección procederán a su apagado controlado.

El Responsable del Sistema deberá verificar que anualmente se revisa la capacidad de los SAI, con el objetivo de detectar limitaciones que puedan suponer un riesgo para el servidor y proceder a su sustitución en caso necesario.

4.4. Seguridad del cableado

Es necesario proteger contra daños o interceptaciones los cables de energía y telecomunicaciones, para lo cual se cumplirán las siguientes indicaciones:

- Se evitará el paso de cableado de datos a través de zonas públicas o comunes del edificio. Si no es posible evitarlo, se tratarán las comunicaciones que pasen por zonas comunes como externas, aplicándoles las medidas adecuadas.
- El cableado de energía y datos estará debidamente canalizado para evitar intercepciones o daños.
- Los paneles de acceso a puntos de conexión tanto de energía como de datos estarán debidamente cerrados y/o precintados para evitar las manipulaciones no autorizadas.

4.5. Mantenimiento de equipos

Se establecerán pautas de mantenimiento para los equipos de la Organización, de forma que se asegure su disponibilidad e integridad. En cuanto a las tareas de mantenimiento de equipos, además de lo indicado en el PR-10 **Mantenimiento**, la Organización establece las siguientes:

- Revisión conforme a lo establecido por la ley de los sistemas de extinción.
- Revisión anual de la capacidad de los SAI.
- Limpieza, aspirado y revisión anual de los sistemas de ventilación de equipos y servidores.

Las labores de mantenimiento realizadas se anotarán en las correspondientes fichas de equipo.

Para el resto de equipos no detallados en este punto, se aplicarán las revisiones o labores de mantenimiento especificadas por el fabricante.

Las tareas de mantenimiento deberán realizarse únicamente por personal autorizado y con la capacidad técnica necesaria para llevarlas a cabo.

4.6. Seguridad fuera de las instalaciones

A la hora de utilizar cualquier equipo de tratamiento o almacenamiento de información fuera de las instalaciones de la Organización, se tendrán en cuenta las siguientes obligaciones por parte de todos los empleados:

- Sólo el personal autorizado podrá utilizar portátiles o teléfonos móviles de empresa, fuera de las instalaciones. Se considerará que existe autorización cuando el activo correspondiente figure en el Listado de Equipos, de lo contrario deberá existir una autorización expresa.
- Los equipos portátiles dispondrán de **contraseñas de acceso** según la política de contraseñas establecida para la Organización, con el fin de proteger la información en ellos contenida y evitar accesos no autorizados a la misma en caso de robo o pérdida.
- Cuando se saque información confidencial en dispositivos de almacenamiento portátil (CD/DVD, llaves USB, discos duros externos, etc.), la información deberá ir **cifrada o protegida por contraseña**.

- Los equipos o medios que se utilicen fuera de las instalaciones serán responsabilidad del empleado quien deberá:
    - Respetar las medidas de seguridad establecidas para los equipos dentro de las instalaciones.
    - Custodiar y vigilar el equipo en lugares públicos, y transportarlo siempre como equipaje de mano.
    - Proteger el equipo debidamente mediante los maletines o fundas correspondientes.
- No estará permitido el uso de **redes públicas** (WIFI) para el trabajo desde fuera de las instalaciones, salvo cuando la dirección de la Organización de autorización expresa para ello.

4.7. Reutilización o eliminación de equipos

Es necesario proteger la información también en el momento de reutilizar o eliminar equipos. Para ello, se seguirán las siguientes instrucciones:

- **Equipos portátiles, PC's o servidores**: Se revisarán antes de su eliminación o reparación fuera de las instalaciones de la Organización para asegurar que se han retirado todos los medios de almacenamiento (CD's, USB's, discos duros, etc.) o que se han sobre-escrito debidamente con herramientas de borrado seguro.
- Los **dispositivos con información confidencial** (CD's/DVD's, llaves USB, discos duros extraíbles, etc.) serán físicamente destruidos o la información contenida en ellos será debidamente eliminada mediante la utilización de herramientas de borrado seguro.
- **Teléfonos móviles**, antes de desecharlos se procederá al borrado de toda la información que puedan contener.

4.8. Retirada de materiales propiedad de la empresa

Antes de que cualquier empleado pueda retirar un equipo o dispositivo con **información confidencial** fuera de las instalaciones, deberá solicitar la correspondiente autorización de la Dirección, siempre y cuando el dispositivo no figure como un activo del empleado y la información extraída no sea la propia de trabajo del empleado.

Para la retirada de materiales fuera de la empresa se deberán tener en cuenta las normas establecidas en el apartado 4.6 de esta Política.

La Dirección o el Responsable del Sistema podrán hacer revisiones inesperadas para detectar la retirada de equipos no autorizada.

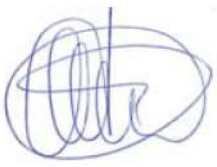
POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	25/03/2020	Emisión inicial
01	09/04/2021	Actualización formato

REVISADO Y APROBADO:

Firma:



Firma Juan Carlos Martínez Rodríguez
Fecha: 09/04/2021

Contenido

1. OBJETO

Establecer los controles y las pautas de trabajo adecuadas en la manipulación y operación de los sistemas de comunicación.

2. ALCANCE

Esta Política es de aplicación a todos los sistemas de comunicación y operación que la organización ponga a disposición de sus trabajadores.

3. RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN

3.1. Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de información, estableciendo las responsabilidades y procedimientos para la gestión y operación de los mismos.

3.2. Procedimientos operativos documentados

Las actividades de los empleados de OPEMAT INGENIERÍA, S.L. en relación a los medios de procesamiento y comunicación deberán seguir las instrucciones establecidas por los fabricantes del hardware y software disponible. En general, la forma de realizar cualquier operación de mantenimiento en los sistemas se estudiará previamente, será autorizada por el **Responsable del Sistema** o por la **Dirección**, y realizada por personal cualificado.

Cuando el **Comité de Gestión de SI** así lo establezca, se desarrollarán procedimientos o instrucciones apropiadas para el manejo, gestión o respuesta a incidentes relacionados con los recursos de tratamiento de información. Los procedimientos o instrucciones operativos documentados que pudieran existir, deberán ser puestos a disposición de los empleados que deban utilizarlos.

El **Comité de Gestión** pondrá especial interés en la posible documentación de las siguientes tareas:

- Realización o recuperación de copias de seguridad.
- Uso de utilidades del sistema.
- Eliminación de soportes y uso de la información.
- Procedimientos de reinicio y recuperación de sistemas tras una caída.
- Monitorización de sistemas.

3.3. Gestión de cambios

Para proceder a la realización de cambios en los sistemas y en los recursos de información de la Organización deberán seguirse las siguientes indicaciones generales:

- Previamente a la realización de cualquier cambio debe salvarse la configuración actual de los sistemas, así como la información que pudiera verse comprometida por el cambio.
- El Responsable del Sistema es el responsable de la instalación de software en los equipos de manera temporal, y la validación de cualquier cambio para que éste sea considerado definitivo.

  La instalación de software, o la realización de cambios en la configuración de los **sistemas críticos (servidores)**, se realizará de acuerdo a las siguientes consideraciones:

- Previamente a la realización de cualquier cambio debe salvarse la configuración actual de los sistemas, así como la información que pudiera verse comprometida por el cambio.
- Si una vez aplicado el cambio se observa algún mal funcionamiento se utilizará la copia del sistema en el momento anterior al cambio para volverlo a su estado anterior válido.

Al igual que para el software "crítico", cualquier cambio significativo en los sistemas de procesamiento de información (instalación de nuevos equipos, servidores, dispositivos, cambios de configuración, etc.) deberán ser probados en un entorno aislado con el objetivo de garantizar que no comprometen la seguridad de la información.

3.4. Segregación de tareas

En las **Fichas de Perfil Puesto** de la Organización se establecen las funciones y responsabilidades en materia de seguridad que cada uno de los empleados. Adicionalmente, en todos los procedimientos del SG, así como en los procedimientos o instrucciones operativas se deberán definirse los responsables de realización de cada tarea.

Las directivas de seguridad aplicadas dentro de los sistemas de información deberán tener en cuenta y garantizar las restricciones establecidas en las fichas de personal y en los perfiles de puesto.

En todo caso, la manipulación y realización de cambios sobre los sistemas de información de la Organización únicamente debe realizarla personal especializado y autorizado para tal tarea.

3.5. Separación de los recursos de desarrollo, prueba y operación

Para el caso concreto de esta organización, no aplica este punto ya que no se realiza desarrollo de software.

4. GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS

4.1. Objetivo

Implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio en consonancia con los acuerdos de provisión de servicios por terceros.

4.2. Provisión de servicios

De cara a la provisión de servicios prestados por terceros, la Organización deberá exigir al tercero cuándo así lo estime oportuno, la documentación o registros que especifiquen:

- Los niveles de seguridad acordados.
- La definición del servicio y de los niveles de entrega incluidos.
- Las posibles herramientas de control del servicio.

4.3. Supervisión y revisión de los servicios prestados por terceros

En casos concretos, y cuando la Organización lo considere oportuno se establecerán mecanismos de monitorización de los servicios prestados por terceros.

Para ello, se procederá de alguna de las siguientes formas:

- Registro y monitorización de las incidencias relativas al servicio, de tal forma que se pueda tener un histórico de los incumplimientos del prestador del servicio a fin de tramitar las reclamaciones o modificaciones que se consideren necesarias.
- Solicitud de informes de cumplimiento de los niveles del servicio, siempre y cuando el prestador del servicio esté dispuesto a facilitar dicha información, o cuándo esta circunstancia haya sido contemplada en el contrato pertinente.
- Monitorización del servicio a través de herramientas automatizadas, siempre y cuando el prestador del servicio las ponga a disposición de la Organización.

De forma anual se revisará que los compromisos adquiridos por los terceros se cumplen y que garantizan los niveles de seguridad adecuados al servicio prestado.

La información proporcionada por terceros para su supervisión, será debidamente almacenada por si esta fuera necesaria para la realización de inspecciones o auditorías.

4.4. Gestión de cambios en los servicios prestados por terceros

Cuando se produzcan cambios en la provisión de los servicios facilitados por terceros, deberá analizarse el impacto de los mismos sobre los activos y sistemas de información propios. Si se

considera oportuno, fruto de la implantación de los cambios en los servicios prestados, debería realizarse una reevaluación de los riesgos.

5. PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA

5.1. Objetivo

Minimizar el riesgo de fallos de los sistemas y recursos empleados por la Organización.

5.2. Gestión de capacidades

Con una periodicidad anual se revisará la capacidad de los sistemas de la Organización para detectar posibles necesidades de ampliación de los mismos, así como anticiparse a las futuras necesidades de capacidad que garanticen el comportamiento requerido de los sistemas.

5.3. Aceptación del sistema

Previamente a la aceptación e implantación de nuevos sistemas de información, se deberán establecer las pruebas de operación y seguridad que dichos sistemas deberán cumplir, sometiéndolos a dichas pruebas en entornos controlados antes de pasarlos a funcionamiento en el entorno real.

6. PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y DESCARGABLE

6.1. Objetivo

Implantar medidas de protección para prevenir y detectar la introducción de software malicioso y códigos móviles no autorizados.

6.2. Control contra código malicioso

Para protegerse contra las amenazas provocadas por código malicioso la Organización establece las siguientes medidas:

- Instalación de software antivirus en cada uno de los equipos.
- Instalación y gestión de un firewall por hardware crítico para evitar accesos no deseados.

Además de las medidas anteriores, todos los empleados de la Organización seguirán las siguientes pautas de actuación:

- Evitar la descarga de archivos de sitios que no sean de confianza o de los que no se conoce el origen.
- No se podrá instalar ningún software que no esté autorizado por el Responsable del Sistema de la organización.

- Escaneo de todos los dispositivos externos que puedan contener código malicioso (llaves USB, CD's, etc.) antes de permitir su exploración desde el equipo local.
- Comprobación de los adjuntos y descargas de los correos electrónicos. Para ello se utilizará la función de protección en tiempo real de correo del antivirus instalado.
- Asegurarse de que el software antivirus se encuentra vigente y correctamente actualizado.

  Además, el Responsable del Sistema estará atento a la aparición de nuevas amenazas que puedan comprometer la seguridad del sistema para ello estará subscrito a boletines, foros especializados, etc.

7. COPIAS DE SEGURIDAD

7.1. Objetivo

Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

7.2. Copias de seguridad de la información

La Organización definirá una **Política de copias de seguridad** acorde a las necesidades de la empresa. En la **Política de copias de seguridad** deberá especificarse el tipo y frecuencia de las copias realizadas, el responsable de realización de las copias y el método y responsables de verificación de las mismas.

8. GESTIÓN DE LA SEGURIDAD EN REDES

8.1. Objetivo

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

8.2. Controles de red

La configuración y mantenimiento de la red es responsabilidad del Responsable del Sistema. Los controles de acceso a redes se realizan de acuerdo a lo establecido en la **Política de Control de Acceso**, en su punto **6-Control de acceso a redes.**

8.3. Seguridad de los servicios de red

Para todos aquellos servicios de red que la Organización ponga a disposición de sus empleados o de sus clientes deberán tenerse en cuenta las siguientes medidas de seguridad:

- Cuando se disponga de Intranet, Wiki, ERP, CRM, gestores de proyectos, o cualquier otra herramienta colaborativa, se deberán establecer un acceso y uso controlado por usuario y

contraseñas, de tal manera que cada usuario acceda únicamente a la parte del recuso que necesite para su trabajo.

- Los recursos compartidos de red solo estarán accesibles a aquellas personas que los necesiten para su trabajo.
- En caso de existir redes Wifi, estas deberán estar protegidas con claves de seguridad robustas, tener un acceso limitado a los recursos de la Organización y cuando sea posible deberían estar en una red independiente.

9. MANIPULACIÓN DE SOPORTES

9.1. Objetivo

Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la Organización.

9.2. Gestión de soportes extraíbles

Es necesario proteger la información que se desplaza físicamente fuera de las dependencias propiedad de la Organización. Para ello se seguirán las siguientes pautas:

- Equipos portátiles: Los equipos portátiles no podrán contener información confidencial alguna, salvo aquella autorizada por la dirección de OPEMAT INGENIERÍA, S.L. y siempre que esta información vaya cifrada o protegida por contraseña.
- Dispositivos de almacenamiento (CD's, DVD's, llaves USB's, discos duros portátiles, etc.): Queda prohibida la extracción de información confidencial o interna mediante alguno de estos medios sin autorización de la Dirección y sin el uso de las técnicas de cifrado o de encriptación adecuadas a la información que contengan.

Siempre que se autorice el uso de soportes extraíbles y éstos contengan información confidencial o de alto valor para la Organización, dicha información deberá ir cifrada.

9.3. Retirada de soportes

La eliminación de medios debe hacerse de forma segura y sin peligro cuando no se necesiten más, asegurando que la información confidencial que contenga sea destruida completamente. Para ello se deberá seguir lo estipulado en la Política de Seguridad física y ambiental en su apartado Retirada o eliminación de equipos.

En cuanto a la información que no esté en soportes digitales se tendrá en cuenta las siguientes consideraciones:

- La documentación impresa que contenga información confidencial o de uso interno deberá ser destruida empleando una trituradora de papel.
- Cuando el volumen de información en formato impreso sea elevado, podrá considerarse la posibilidad de contratar a una empresa que se encargue de la recogida y destrucción de la información.

9.4. Procedimiento de manipulación de la información

Para la manipulación de la información se seguirán las pautas establecidas en el procedimiento PR-01 Control de la documentación y los registros y en la Política de Gestión y clasificación de la información.

9.5. Seguridad de la documentación del sistema

La documentación del sistema de gestión está clasificada como información de uso interno, por lo que seguirá las pautas de manipulación marcadas para este tipo de información en el procedimiento PR-01 Control de la documentación y los registros y en la Política de Gestión y clasificación de la información.

10. INTERCAMBIO DE INFORMACIÓN

10.1. Objetivo

Mantener la seguridad de la información y del software intercambiado dentro de la organización y con cualquier otra entidad externa.

10.2. Políticas, procedimientos y convenios de intercambio de información

El intercambio de información seguirá las pautas establecidas en el procedimiento PR-01 Control de la documentación y los registros y en la Política de Gestión y clasificación de la información, para cada una de las categorías de información establecidas.

Cuando sea necesario, debido a la naturaleza de la información en tránsito, la Organización establecerá los contratos de confidencialidad o convenios de intercambio, que regulen el procedimiento de intercambio correspondiente. En estos contratos o convenios deberán establecerse las pautas para:

- Notificación y transmisión de información.
- Responsabilidades ante incidentes de seguridad (pérdidas, destrucción, deterioro, etc.) de la información.
- Mecanismos o técnicas de identificación o etiquetado.
- Métodos criptográficos o de cifrado a emplear.
- Etc.

10.3. Soportes físicos en tránsito

Las condiciones para el transporte o envío físico de información son los siguientes:

- Dispositivos de almacenamiento portátiles o extraíbles: se seguirá lo indicado en el apartado 0 Gestión de soportes extraíbles de esta Política.
- Dispositivos de almacenamiento de copias de seguridad: se seguirá lo descrito en el apartado 0 Copias de Seguridad de la presente Política.
- Información en formato papel: se seguirán las pautas establecidas en la Política de Gestión y clasificación de la información, en el apartado de Etiquetado y manipulado de la información.

  Para realizar el cifrado de los soportes de información se podrán utilizar, por ejemplo, las siguientes herramientas gratuitas:
- Rohos Mini Drive (http://www.rohos-es.com/productos/rohos-mini-drive/)

10.4. Mensajería electrónica

Cuando sea necesario el envío de información crítica a través de sistemas de mensajería electrónica, se aplicarán en la medida de lo posible las siguientes medidas de seguridad:

- Envío de ficheros cifrados o protegidos por contraseña.
- Envío de documentos en formato pdf para evitar la alteración del contenido.
- Comprobación de la lista de remitentes antes del envío del mensaje para evitar enviar información crítica a destinatarios incorrectos.

Cuando no sea factible la aplicación de las medidas mencionadas, se incluirán en la comunicación electrónica las indicaciones oportunas para el manejo seguro de dicha información.
Todos los mensajes electrónicos irán acompañados de los correspondientes avisos legales de seguridad y confidencialidad de datos.

10.5. Sistemas de información empresarial

Los sistemas de información empresarial deberán cumplir con los requisitos impuestos a los servicios de red en el apartado 9.3 de esta Política, se deberá prestar especial atención a:

- Aplicaciones de contabilidad, facturación o intercambio de datos financieros y contables. El uso de estas herramientas estará restringido por usuarios, teniendo acceso cada usuario únicamente a las funcionalidades que necesite para su trabajo.
- Uso correo postal. La información recibida por correo postal deberá ser entregada a su destinatario que será el autorizado a su apertura.

11. SERVICIOS DE COMERCIO ELECTRÓNICO

11.1. Objetivo

Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos.

11.2. Transacciones en línea

Este punto no resulta de aplicación en la organización. Sin embargo, se deja especificado un pequeño resumen de lo que sería necesario.
Se tendrán en cuenta las siguientes consideraciones:

- Siempre se utilizarán comunicaciones encriptadas.
- Solo se podrán hacer compras o pagos a proveedores aprobados.
- Cuando se vaya a realizar el pago se comprobará la información de seguridad facilitada por el navegador (uso de conexiones https, y páginas firmadas por organismos de confianza como por ejemplo VeriSign), comprobando que se trata de una página segura.
- Nunca se realizarán pagos desde ubicaciones inseguras (sitios públicos o redes Wifi no seguras), quedando limitadas las operaciones electrónicas a las instalaciones de OPEMAT INGENIERÍA, S.L.
- Una vez realizadas las transacciones electrónicas se comprobarán los cargos hechos en la cuenta bancaria para constatar que todo es correcto.

11.3. Información puesta a disposición pública

En la actualidad no existen sistemas públicos de intercambio de información dentro del alcance de la certificación, aunque si hay un sitio Web con información comercial. Periódicamente se revisará la información puesta a disposición pública a través de la Web para verificar que es correcta.

Siempre que en la organización se realice algún cambio en la documentación o a nivel organizacional que afecte a la información publicada, se revisará convenientemente para garantizar su exactitud.

12. USO ACEPTABLE DE LOS ACTIVOS

El uso generalizado de los sistemas de información de los usuarios de la red de OPEMAT INGENIERÍA, S.L. en el desarrollo diario de su labor, hace imprescindible que todos los trabajadores sean conscientes de su responsabilidad en el uso de estos sistemas y en la protección de la información accesible en ellos y a través de ellos.

Los sistemas de información y la información deben ser utilizados para fines exclusivamente laborales, para los que han sido puestos a disposición de los usuarios.

En general, no se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red o los sistemas de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Instalar, modificar o cambiar la configuración de los sistemas de software
- Utilizar los equipos y recursos para fines personales.
- Introducir virus u otras formas de software malicioso de forma intencionada. Antes de utilizar cualquier medio de almacenaje de información, se debe comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda molestar u ofender.

A continuación, se especifica detalladamente la Política de Uso Aceptable de cada uno de los entornos a los que aplica.

(a) SERVIDORES

En la definición de esta Política se considera SERVIDOR a un ordenador o máquina virtual (software que emula a un ordenador) que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

En esta Política se incluyen tanto las normas de utilización del acceso a recursos, aplicaciones o información específica como las normas de administración y gestión de servidores por parte de usuarios administradores de servidores departamentales concretos.

NORMATIVA

Uso general

- El acceso en red a los servidores y sus recursos está destinado a fines exclusivamente laborales, no se permite el almacenamiento personal que no se refiera a los datos de clientes o documentación de cada departamento.

- El acceso de un usuario a los recursos específicos y aplicaciones de los servidores se definen en función del perfil o puesto de trabajo que éste desempeña. Es responsabilidad del propio

usuario no malgastar intencionadamente los recursos de la red o destruir datos de otros usuarios a los que tenga acceso.

- Utilizar las unidades de red establecidas para toda la organización como repositorio de información. Se trata de unidades a las que se accede a través de un medio de autenticación seguro, protegidas por permisos de acceso establecidos en función del trabajo encomendado a cada trabajador y objeto de copias de seguridad periódicas que garantizan su disponibilidad ante eliminación involuntaria o corrupción de información.

- Fuera del horario laboral, no debe quedar ninguna sesión o fichero abierto en el servidor, a fin de poder hacer cualquier instalación, copia de seguridad o mantenimiento del mismo.

- Los usuarios que, por su puesto de trabajo, dispongan de una contraseña que les permita administrar y/o gestionar por escritorio remoto cualquier servidor son responsables de su uso, no permitiéndose ningún cambio ni de configuración, ni del registro del sistema, ni de instalación de software sin antes consultarlo con personal del departamento informático.

- Existen aplicaciones puestas a disposición de determinados usuarios a través de escritorio remoto. El uso de estos accesos se restringe a la ejecución de dicha aplicación, debiendo cerrarse correctamente para no dejar sesiones activas en el servidor que puedan tener efectos negativos en el rendimiento o en posibles tareas de mantenimiento en el mismo.

Protección de la información

- El acceso a los recursos y aplicaciones se concede individualmente (o mediante pertenencia a grupos de usuarios) y se realiza a través de un medio de autenticación seguro. Es responsabilidad del usuario garantizar un uso adecuado de su identificador y contraseña.

- La contraseña de acceso al dominio es un dato privado del usuario que, bajo ningún concepto, debe dar a conocer. Por razones de seguridad, se recomienda una contraseña consistente, con al menos 6 caracteres, combinando letras, número y caracteres especiales, y evitando palabras concretas. Debe ser cambiada siempre que se tenga sospecha de que otras personas puedan tener conocimiento de la misma, no obstante, se recomienda el cambio periódico.

- El cambio de contraseña, para entornos Microsoft Windows, puede hacerse de manera sencilla pulsando simultáneamente Ctrl+Alt+Supr y seleccionando la opción “cambiar contraseña”.

Configuración e instalación

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

Mantenimiento y tratamiento de incidencias

- En caso de borrado accidental de archivos o movimiento de carpetas en servidores, se debe informar inmediatamente al Responsable del SG.
- Cualquier incidencia (problema o mal funcionamiento) o anomalía (comportamiento extraño o inesperado) en el acceso a un servidor se debe notificar lo antes posible al Responsable del SG.

RECOMENDACIONES

- En caso de acceso por escritorio remoto a cualquier servidor departamental (usuarios administradores de servidores específicos) se recomienda no navegar por Internet ni descargar software, actualizaciones o parches. Es aconsejable realizar las búsquedas y descargas desde una estación de trabajo y hacerlas llegar al servidor a través de la red interna.
- Es recomendable que todos los servidores o equipos de propósito específico no configurados como miembros del dominio interno configuren en su sincronización horaria contra un servidor NTP externo de forma que su fecha y hora sea fiable e idéntica al resto de equipamiento de la red. Los servidores centrales están sincronizados contra una fuente externa, el resto de equipos que pertenecen al dominio se sincronizan con estos servidores centrales

CONTROL

Por razones de seguridad y rendimiento, OPEMAT INGENIERÍA, S.L. se reserva el derecho de monitorizar, auditar y mantener trazas de las acciones llevadas a cabo por los usuarios en los sistemas informáticos, así como realizar acciones de mantenimiento sobre los equipos que pueden estar causando problemas de rendimiento o mal funcionamiento de los diferentes elementos que configuran la infraestructura de TI.

(b) CORREO

Todo correo electrónico emitido bajo dominio tutelado o titularidad de OPEMAT INGENIERÍA, S.L. puede ser considerado por el receptor como un comunicado oficial y, por tanto, se debe tener el máximo cuidado en los contenidos de los mensajes.

Sin embargo, el hecho de disponer de una cuenta de correo electrónico bajo dominio tutelado o titularidad de OPEMAT INGENIERÍA, S.L. no autoriza al emisor a representar a OPEMAT INGENIERÍA, S.L. o actuar en su nombre más allá de su habilitación específica o por razón de su cargo.

OPEMAT INGENIERÍA, S.L. no se hace responsable del contenido de los mensajes en caso de acciones penales o civiles contra el emisor(es) del mensaje(s) emitido(s).

NORMATIVA

Uso general

- El uso del correo de OPEMAT INGENIERÍA, S.L. se limita al ámbito profesional, de modo que solo se debe utilizar para el cumplimiento de las tareas y funciones asignadas. No se puede hacer uso del mismo en el ámbito personal ni configurar cuentas personales en el software de correo estándar.

- En función del perfil o puesto de trabajo que desempeña el usuario, éste tiene definidos unos límites específicos de almacenamiento de buzón, de tamaño de envío y recepción de mensajes y un número máximo de mensajes a enviar. Es responsabilidad del propio usuario realizar las tareas de revisión y de depuración periódicas que permitan mantener su buzón en correcto funcionamiento sin superar los límites establecidos.

- Se debe incorporar una despedida y una firma al pie del correo con información suficiente para establecer en todo momento quién es el emisor del mensaje dentro de OPEMAT INGENIERÍA, S.L. y cuáles son sus datos de contacto.

- En cuanto a las listas de distribución corporativas, su uso debe limitarse al envío de comunicaciones internas relevantes que sean imprescindibles para el mantenimiento y la mejora de la organización, provenientes de la Dirección o del personal autorizado de los distintos departamentos.

- Cuando se reenvía un mensaje, no se debe manipular el contenido de la información del mensaje original y enviarlo tal y como fue recibido. En las ocasiones en que el reenvío se utiliza para entremezclar una respuesta, es necesario informar de las modificaciones del mensaje original dejándolas claramente identificadas.

Usos inaceptables

Se prohíbe utilizar el correo electrónico para crear o enviar:

- Mensajes con contenido ofensivo, obsceno, poco ético, amenazador, de calumnia o que pueda suponer merma de la imagen y consideración de OPEMAT INGENIERÍA, S.L. y los que la componen.

- Cualquier actividad lucrativa o comercial de carácter individual, privado o para negocio particular.

- Difusión interna o externa de correo no deseado (spam), sea o no masiva, de virus y otro código malicioso, así como para el envío de cartas en cadena.

- Envío de información que no sea de carácter laboral.

Protección de la información

- El acceso al correo desde el exterior debe hacerse de forma adecuada. OPEMAT INGENIERÍA, S.L. pone a disposición del personal autorizado el acceso por Internet mediante web-mail y, en función del tipo de trabajador, otras opciones de conexión segura como acceso a la red por VPN.

- En cualquiera de los casos, se deben extremar las medidas de precaución eliminando los archivos temporales de los navegadores utilizados una vez finalizada la sesión y evitando dejar sesiones abiertas visibles a terceros ajenos a OPEMAT INGENIERÍA, S.L. En ningún caso hacer uso del guardado de contraseñas que suelen poseer dichos navegadores.

- Se debe adjuntar de forma estándar al pie del correo (o firma) una cláusula para proteger la posible confidencialidad de la información contenida en el mensaje.

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

- En caso de archivado o exportación del buzón de correo es necesario guardar los ficheros resultantes en una ubicación que ofrezca garantías suficientes de confidencialidad de la información que ellos contienen. Se recomienda informar al Responsable del SG para que pueda almacenar en sus sistemas de respaldo una copia del archivado como medida de protección.

Acceso a buzones de correo (cuenta email)

- El acceso a los buzones de correo se concede individualmente y se realiza a través de un medio de autenticación seguro. Es responsabilidad del usuario garantizar un uso adecuado de su identificador y contraseña. En caso de que, de forma temporal o permanente, sea necesario que otras personas accedan a nuestro buzón, ya sea solo para la lectura o para leer y enviar mensajes en nuestro nombre, nunca se debe realizar dándoles a conocer nuestras credenciales de acceso, sino que se debe hacer a través de las opciones de "Delegación de acceso" (por ejemplo, a través del asistente de "Fuera de oficina"). De no ser posible, otra opción para permitir la lectura es reenviar el correo hacia el buzón de la otra persona, cuando este buzón sea interno a OPEMAT INGENIERÍA, S.L. y bajo petición expresa del Responsable del SGSI para su estudio y tramitación.

- Por razones de seguridad, está prohibido activar las opciones de "Recordatorio de contraseña" para acceder a los buzones, aunque esto conlleve la necesidad de autenticarse cada vez que se activa el envío y recepción de mensajes.

Mailings o envíos masivos

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

Mantenimiento y tratamiento de incidencias

- Cualquier incidencia (fallo o mal funcionamiento) o anomalía (comportamiento extraño o inesperado) del correo se debe notificar lo antes posible al Responsable del SG.
- Los incidentes de seguridad (pérdida de equipamiento o de datos que puedan facilitar a terceros el acceso al buzón), deben ser comunicados al Responsable del Sistema. De acuerdo a lo descrito en el procedimiento PR-03 Gestión de no conformidades y acciones correctivas.
- Tanto las estaciones de trabajo como los servidores de correo y los firewall de acceso están dotados de software antivirus. No obstante, se recomienda abstener se abrir correos sospechosos procediendo a su borrado inmediato o contactando con el Responsable del SG en caso de duda.
- Si se tiene la sospecha de infección por virus u otro código malicioso, no usar el correo para evitar su propagación y proceder de inmediato a informar al Responsable del SG, al tratarse de una incidencia de seguridad de carácter grave.

RECOMENDACIONES

Uso general

- Leer el correo frecuentemente, al menos una vez al día.
- Eliminar mensajes innecesarios.
- No suscribirse a listas de correo por Internet a menos que sea estrictamente necesario. Esto provoca que lleguen a su buzón gran cantidad de mensajes de correo provocando saturación.

Sobre el contenido

- Escribir en el "Asunto" una palabra o frase que ayude al receptor a saber de qué se trata el mensaje y le permita filtrarlo, priorizarlo, archivarlo y, más adelante, recuperarlo.
- Escribir los mensajes bien formateados. Las personas que reciben el correo pueden no leer un mensaje mal formateado. Revisar la correcta redacción y la ortografía.
- Escribir los mensajes con lenguaje profesional, no ser demasiado informal o coloquial. No escribir nada que no se sea recomendable dejar por escrito. Ser neutral y evitar lenguaje sarcástico, sexista, insultante, abusivo o discriminador, que pudiera ofender o irritar a los demás.

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

- Para evitar sobrecarga de la red, no adjuntar imágenes o archivos de gran volumen al mensaje (ficheros con imágenes, fotos, presentaciones, etc.).

Sobre el envío de mensajes

- Antes de enviar el mensaje, revisar el texto que lo compone y los destinatarios con el fin de corregir errores de ortografía, forma o fondo.

- Antes de enviar un mensaje a una lista de distribución es preciso analizar si no existen otras herramientas de comunicación masiva (boletines, intranets, etc.). Es necesario analizar si realmente todos los miembros de la lista están interesados en ese mensaje.

- Dirigir el mensaje (campo "Para:") a las personas de las que se espera una acción o respuesta. Enviar copias (campo "CC" / "CCO") a las personas que desea mantener informadas, pero de las que no se espere ninguna acción o respuesta.

- Al contestar un mensaje, incorporar el cuerpo del mensaje al que corresponde para mantener intacta la cadena de información.

- Antes de reenviar un mensaje, asegurarse de que toda la información que está reenviando puede ser desvelada al destinatario.

- Utilizar las opciones de seguimiento de los mensajes enviados (acuse de recibo, etc.) solo cuando realmente sea necesario.

- No contestar nunca a mensajes de spam, ni responder a la opción de "dar de baja la suscripción" de estos mensajes, para evitar dar a conocer a los emisores del spam que se trata de una dirección de correo válida, y evitar así que puedan intensificar el envío de correo basura.

- Para enviar información confidencial a través del correo electrónico, es recomendable utilizar medios de seguridad adicional, pues el correo en sí mismo no es un medio de comunicación seguro. Cuando se disponga de certificado digital y se tenga la certeza de que el receptor podrá descifrar el mensaje, se recomienda usarlo. En caso de no disponer de certificado digital, es posible proteger los archivos que contienen la información utilizando, por ejemplo, las opciones de protección con contraseña que incluyen algunos programas ofimáticos.

- Si no tiene tiempo de contestar los mensajes completamente, envíe un breve mensaje de forma tal que la persona que le envió el mensaje sepa que usted lo recibió y que tiene pendiente responderle.

Retención de correo

- Es recomendable ser selectivos a la hora de almacenar correos y guardar solo aquellos que puedan ser útiles en el desarrollo del trabajo. No guardar mensajes de manera sistemática y permanente y hacer revisiones de depuración periódica.
- Es una práctica extendida realizar archivados o exportaciones del buzón de correo para no sobrepasar el límite de almacenamiento del mismo y para contribuir al correcto funcionamiento de los sistemas centrales.

En caso de ausencia de la oficina

- Se recomienda notificar las ausencias de la oficina (vacaciones, etc.) con antelación suficiente al personal implicado o relacionado con nuestra labor.
- En caso de ausencia por más de un día, utilizar la opción "Fuera de oficina", indicando el primer y último día de ausencia, para notificar a las personas que nos envían mensajes hasta cuándo estaremos ausentes y con quién pueden contactar en caso de urgencia.

CONTROL

Por razones de seguridad, para garantizar el buen funcionamiento de los sistemas de correo electrónico, OPEMAT INGENIERÍA, S.L. se reserva el derecho de monitorizar el origen y el destino de los mensajes de correo electrónico y el volumen de correo electrónico enviado y recibido. Nunca se accederá y/o revelará el contenido de los mensajes, salvo que sea por motivos de seguridad fundamentados o requerimiento legal, debiendo dar cumplimiento en estos casos a los procedimientos legales establecidos.

(c) CONEXIÓN A INTERNET

En general, todos los usuarios con acceso a la red corporativa de OPEMAT INGENIERÍA, S.L. tienen acceso a este servicio.

El usuario es totalmente responsable del uso que realice del mismo y de los sitios visitados teniendo en cuenta los puntos siguientes:

NORMATIVA

Uso general

- El uso de la conexión a Internet de OPEMAT INGENIERÍA, S.L. se limita al ámbito profesional, es decir, que solo se debe utilizar para el cumplimiento de las tareas y funciones asignadas.

Se consideran usos aceptables, siempre que se den dentro del ámbito laboral:

- Comunicación entre empleados y entidades/personas externas a la organización.
- Consulta a webs de soporte de productos, información técnica, información comercial, etc.
- Descarga de productos, actualizaciones de productos, parches, etc., relacionados con la actividad laboral determinada y siempre dentro del ámbito legal correspondiente.

- A nivel de organización, existen una serie de filtros generales que restringen parcialmente el acceso a determinados contenidos no deseados o peligrosos a efectos de evitar las posibles consecuencias negativas que estos accesos puedan implicar en los sistemas de información centrales. Esto no exime al usuario de su responsabilidad ante el uso inadecuado del servicio y ante el acceso a contenidos no recomendables que puedan, por cualquier causa, traspasar estos filtros.
- Queda prohibida la descarga de cualquier tipo de software pirata, contenidos sin permisos del autor o material protegido por propiedad intelectual, acuerdos de licencia, etc.

Usos inaceptables

Se prohíbe utilizar la conexión a Internet para:

- Realizar cualquier actividad lucrativa o comercial de carácter individual, privado o para negocio particular.
- El acceso a lugares e información ilegales, obscenos, que distribuyan material pornográfico, o bien materiales ofensivos en perjuicio de terceros por razones de raza, sexo, condición social, etc.
- El acceso a servicios particulares como redes sociales y demás servicios similares.
- Difusión de información confidencial interna o externa de la organización.
- Difusión interna o externa de virus y otro código malicioso.
- Utilizar los recursos para ganar acceso no autorizado a redes y sistemas remotos.
- Provocar deliberadamente el mal funcionamiento de ordenadores, estaciones o terminales periféricos de redes y sistemas.

Mantenimiento y tratamiento de incidencias

Cualquier incidencia (fallo o mal funcionamiento) o anomalía (comportamiento extraño o inesperado) del servicio de acceso a Internet se debe notificar lo antes posible al Responsable del SG.

RECOMENDACIONES

- Restringir el acceso a Internet a sitios conocidos. No navegar por páginas totalmente desconocidas, dudosas o en enlaces contenidos en correos electrónicos sospechosos. Prestar atención al resumen y URL resultado de búsqueda de contenidos en Internet antes de acceder a los mismos.
- No dejar desatendidos los ordenadores mientras están conectados.
- No aceptar la ejecución de programas cuya descarga se active sin que nosotros lo solicitemos.
- No descargar/ejecutar ficheros desde sitios sospechosos porque pueden contener código potencialmente malicioso. Analizar con un antivirus todo lo que se descarga antes de ejecutarlo en tu equipo.
- Descargar programas desde los sitios oficiales para evitar suplantaciones maliciosas.
- Realizar descargas de gran volumen fuera del horario laboral para evitar impacto negativo en el rendimiento del sistema.

CONTROL

Por razones de seguridad, para garantizar el buen funcionamiento de los sistemas de acceso a Internet, OPEMAT INGENIERÍA, S.L. se reserva el derecho de monitorizar el origen y el destino de los accesos y el volumen y contenido de la información enviada y recibida.

(d) ESTACIONES DE TRABAJO

Entendemos por estación de trabajo el equipo informático y accesorios a través de los cuales el usuario accede habitualmente a la información, aplicaciones y sistemas de información necesarios para el desarrollo habitual de sus funciones.

Esta Política afecta a todos los usuarios de OPEMAT INGENIERÍA, S.L.:

- Tanto si la utilización del equipo es exclusiva como si es compartida entre diferentes usuarios.
- Tanto si la estación de trabajo se conecta a la red interna como si se conecta de forma aislada.
- Tanto si almacena información a nivel local como si accede a la información a través de la red.

NORMATIVA

Uso general

- La estación de trabajo y el software instalado son herramientas que la organización pone a disposición de su personal para el desarrollo de las funciones encomendadas. Por tanto, el

personal debe abstenerse de realizar cualquier uso que interfiera en el correcto ejercicio de sus tareas y funciones o en el normal funcionamiento de las instalaciones informáticas. El uso de los equipos está reservado para fines exclusivamente laborales. Nunca se debe utilizar la estación de trabajo con propósito ilícito o propósitos no autorizados por OPEMAT INGENIERÍA, S.L.

- Cada usuario es responsable de su equipo y debe velar por su correcto mantenimiento y configuración. El personal debe hacer el uso más apropiado de la estación de trabajo para evitar que ésta sea dañada o manipulada.

- Al arrancar, la estación de trabajo está configurada para solicitar la autenticación de quien se conecta (identificador, contraseña y dominio al que se accede). Es responsabilidad del usuario mantener las contraseñas en secreto y recomendable utilizar contraseñas consistentes, con al menos 6 caracteres, combinando letras, números y caracteres especiales, y evitando palabras concretas. Debe ser cambiada siempre que se tenga la sospecha de que otras personas puedan tener conocimiento de la misma; no obstante, se recomienda el cambio periódico.

- En caso de que dichas credenciales sean requeridas por el Responsable del SG por razón de sus labores (instalaciones de software, mantenimiento, etc.) se recomienda sustituir a contraseña por una temporal que se suministrará al Responsable del SG para que pueda hacer sus trabajos y volver a cambiarla (volviendo a la anterior si se desea) una vez finalicen los mismos.

- Queda prohibida la conexión a la red interna de la organización de equipos de propiedad del trabajador, salvo que sea previamente verificado y expresamente autorizado por la Gerencia o el Responsable del SG.

- Queda prohibido desactivar o manipular el antivirus corporativo que se ejecuta en cada estación de trabajo. Y, solo en caso justificado, con notificación y aprobación de la Gerencia o del Responsable del SG, se podrá desactivar temporalmente. Es responsabilidad del propio usuario los perjuicios que se puedan derivar por infecciones de virus en su propio equipo o propagadas en la red, en las que se constate que el antivirus estaba desactivado.

- La política de actualizaciones automáticas e instalación de parches de sistema operativo vendrá indicada por las instrucciones que el Responsable del SG marque en cada momento y en cada caso, según considere en beneficio del buen funcionamiento de los sistemas.

- Cuando un usuario cause baja en la empresa debe entregar todo el equipamiento de TI que le fue suministrado para su labor a la Gerencia o a su inmediato superior, en función de la localización del centro de trabajo del usuario y la presencia o no allí de éstos. La persona que recoja el material debe notificarlo al Responsable del SG lo antes posible para facilitar la revisión de inventario y su reutilización.

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

Protección de la información:

- El único recurso para el almacenamiento de la información de los procesos de negocio de la organización son las unidades de red correspondientes. Para evitar accesos indebidos, duplicidades de información, facilitar la compartición de información y garantizar la continuidad de esta información siempre se debe evitar almacenar dicha información en disco local y en soportes externos.

- En caso de que sea indispensable almacenar información – en todo caso de tipo auxiliar – en el disco local o apoyos externos, es necesario tomar medidas adecuadas para proteger la información según el nivel de confidencialidad o criticidad de la misma, protegiéndola siempre de accesos ilegítimos.

  En este caso, es responsabilidad del usuario garantizar la continuidad de esta información, realizando, por ejemplo, copias periódicas en soportes externos, pues cualquier avería, problema del ordenador o acción de mantenimiento, podría suponer la pérdida total o parcial de esta información.

  Es posible contactar con el Responsable del SG para conocer las alternativas existentes con objeto de garantizar la continuidad y confidencialidad de esta información.

- Es necesario tener máximo cuidado en el tratamiento de la información generada en papel, cuidando de dejar siempre la documentación recogida al finalizar la jornada laboral.

  Cuando los datos tratados sean confidenciales o privados, protegidos por la LOPD, se debe guardar la documentación en papel en lugar seguro.

- La estación de trabajo no debe quedar nunca desatendida, especialmente si se ha superado el proceso de identificación y autenticación para acceder a sistemas y/o aplicaciones. Cuando la persona conectada tenga que abandonar el ordenador temporalmente debe bloquear el ordenador (pulsar: tecla Windows + L).

- Es obligatorio mantener habilitado el modo de bloqueo de pantalla con contraseña que se activa tras un tiempo de inactividad (se recomienda 5 minutos).

- El acceso remoto a redes, ya sean controladas o no, tanto si la estación de trabajo está conectada a través de red interna como si no lo está, debe ser previamente autorizado para asegurar el ordenador adecuadamente.

- Está prohibido dar acceso a archivos o carpetas propias a otras personas, a través de las opciones de “Uso compartido” sin la autorización previa de un superior.

- Se debe apagar la estación de trabajo y su monitor al finalizar la jornada laboral.

- No ejecutar software en la estación de trabajo si no se sabe de dónde proviene, ni descargar nada de Internet si no se confía en la web de origen.
- No almacenar contraseñas de acceso a la estación de trabajo, red, aplicaciones, correo electrónico, etc.

Configuración e instalación

- Las estaciones de trabajo se configuran para optimizar la productividad y mantenimiento del parque informático. Por este motivo, está estrictamente prohibido alterar su configuración.
- Está prohibido modificar la configuración de arranque de la estación de trabajo.
- Está prohibido instalar software no autorizado, para evitar el mal funcionamiento o infecciones de otros programas. Cualquier excepción debe ser tramitada a través de la Gerencia o del Responsable del SG y realizada por él o bajo su supervisión en caso excepcional.
- Está prohibida la copia total o parcial del software instalado protegido por leyes de copyright.
- Está prohibido configurar periféricos y dispositivos de comunicación (módems, bluetooth, dispositivos inalámbricos, etc.) sin previa autorización de la Gerencia o del Responsable Informático.

Mantenimiento y tratamiento de incidencias

- La organización está facultada para realizar las tareas de mantenimiento que sean necesarias en las estaciones de trabajo sin aviso previo y para eliminar todos aquellos elementos que, sin tener relación con las funciones a desempeñar en el puesto de trabajo, puedan causar problemas en el normal funcionamiento de los diferentes elementos que configuran la infraestructura de TI.
- En caso de daños en la estación de trabajo, el usuario debe informar inmediatamente a su superior. Asimismo, se debe reportar al Responsable del SG cualquier problema o anomalía detectada (tiempo de respuesta lento, actividad continua del disco duro, desaparición o cambio de ubicación de archivos, etc.), pues puede ser síntoma de infección de virus o mal funcionamiento de algún componente.
- Nunca se deben abrir los ordenadores o dispositivos adyacentes para intentar repararlos

RECOMENDACIONES

- Las estaciones de trabajo deben ubicarse en zonas de acceso controlado, especialmente cuando se trate de estaciones de trabajo desatendidas destinadas al uso compartido.
- Se recomienda no beber o comer cerca de los equipos de tratamiento de la información.

- Las estaciones de trabajo se deberían situar sobre las meses o en soportes específicos. No se deben poner las CPU de los ordenadores directamente sobre el suelo, ni cambiar su orientación inicial.

- Es necesario prestar especial atención a la posición de la estación de trabajo respecto del usuario, la altura de la pantalla, la posición del teclado y la posición corporal que se adopta al sentarse frente al ordenador, pues si no se hace correctamente puede ser motivo de molestias corporales.

CONTROL

Por razones de seguridad y rendimiento, OPEMAT INGENIERÍA, S.L. se reserva el derecho de monitorizar y mantener trazas de las acciones llevadas a cabo por los usuarios en los sistemas informáticos, así como a realizar acciones de mantenimiento sobre los equipos, cuando existan sospechas de la existencia de software sin licencia o no autorizado u otros elementos que, sin tener relación con las funciones a desempeñar en el puesto de trabajo, puedan estar causando problemas de rendimiento o mal funcionamiento de los diferentes elementos que configuran la infraestructura de TI.

(e) PORTÁTILES Y EQUIPAMIENTO MÓVIL

Para los ordenadores portátiles o equipamiento móvil **se aplican las mismas normativas definidas en el apartado anterior para estaciones de trabajo** (uso general, configuración, etc.). No obstante, dado que este tipo de equipos son susceptibles de ser robados o perdidos, surge la necesidad de **dictar normas adicionales específicas** para ellos.

NORMATIVA

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

- Es obligatorio que todos los móviles de la empresa tengan siempre activado el servicio de buzón de voz, para poder dejarles un mensaje en caso de que se encuentren comunicando o se queden sin cobertura.

- No dejar nunca el ordenador o dispositivo móvil desatendido.

- Siempre que sea posible, conectar el ordenador a elementos fijos a través de cableado y no a través de red inalámbrica.

- En ausencias prolongadas (vacaciones, permisos, etc.) del personal, durante las cuales el ordenador no pueda ser utilizado por otras personas, el ordenador y demás equipamiento móvil debe quedar guardado de forma segura.

- Queda prohibido guardar cualquier información confidencial o afectada por la Ley de Protección de Datos Personal y/o datos de clientes. De darse el caso, se realizará por autorización expresa de la Gerencia y bajo supervisión y control del Responsable del SGSI. Cada usuario o departamento que lo utilice debe asegurar que, en caso de pérdida, no se puede acceder a información sensible que pudiera estar almacenada en ellos: encriptación u otros mecanismos.

- Cuando se utilicen ordenadores portátiles en lugares públicos, salas de reuniones u otras áreas fuera del lugar de trabajo habitual es necesario tomar las medidas adecuadas para evitar que personas ajenas puedan visualizar o acceder a la información del ordenador sin autorización.

- El caso de robo o pérdida de portátiles y/o equipamiento móvil (incluidas tarjetas de acceso a las instalaciones, si las hubiera) debe tratarse como incidente de seguridad grave, informando de inmediato a la Gerencia y al Responsable del SGSI. Para el caso concreto de robo, también se puede presentar una denuncia a los cuerpos y fuerzas de seguridad de la nación donde se haya producido.

RECOMENDACIONES

- Cuando el trabajo se desarrolla en instalaciones externas que no ofrecen condiciones de seguridad suficientes es recomendable dotar a los equipos portátiles de dispositivos antirrobo que permitan sujetarlos a elementos fijos.

- Se deberían adoptar medidas especiales de protección física de los equipos cuando estos trabajen en entornos industriales (protectores de teclado, etc.).

(f) IMPRESORAS

Entendemos por impresora aquel periférico o equipo informático a través del cual el usuario imprime texto o gráficos en papel. En este apartado también se incluyen "impresoras multifunción" que son capaces de incorporar funciones adicionales de otros dispositivos tales como escáner, fotocopiadoras, fax, lector de tarjetas de memoria, etc.

Esta Política afecta a todos los usuarios de OPEMAT INGENIERÍA, S.L.:

- Tanto si la utilización de la impresora es exclusiva como si es compartida entre diferentes usuarios.

- Tanto si la impresora se conecta a la red interna como si se conecta a estaciones de trabajo de forma local.

NORMATIVA

Uso general

El uso de las impresoras está reservado a fines exclusivamente laborales.

Protección de la información

Es necesario tener máximo cuidado en el tratamiento de la información generada en papel. Cuando los datos tratados sean confidenciales o privados y la impresión se realice en una impresora de red de uso compartido, el trabajo de impresión debe recogerse lo antes posible del dispositivo y guardarlo en lugar seguro.

En cualquier caso, debe ponerse especial cuidado en recoger siempre la documentación impresa, no dejándola de manera permanente en las impresoras comunes por el doble motivo de confidencialidad (antes expuesto) y de consumo innecesario de papel y de uso de la máquina.

Configuración e instalación

La conexión e instalación de las impresoras debe ser realizada siempre por el Responsable del SG.

Mantenimiento y tratamiento de incidencias

Los usuarios que hagan uso de una impresora concreta son responsables de supervisión de la misma, introduciendo hojas cuando sea necesario o avisando al Responsable del SG en caso de mal funcionamiento o cuando haya que sustituir un tóner u otro componente.

RECOMENDACIONES

- Imprimir solamente aquellos documentos que realmente sea necesario imprimir.
- En la medida de lo posible y si la impresora lo permite, utilizar el modo borrador (o resoluciones bajas de impresión), doble cara y varias páginas por hoja.
- Si se dispone de impresora en color, emplear de forma general la impresión en blanco y negro y utilizar el color solo para ocasiones especiales.
- Realizar los repasos y corrección de errores en pantalla empleando la corrección ortográfica y la vista previa como apoyo. Imprimir, si es necesario, solo la versión definitiva del documento.
- Utilizar las unidades de red y el correo electrónico para hacer llegar información y documentos a otros usuarios o contactos.

CONTROL

Por razones de seguridad y rendimiento, OPEMAT INGENIERÍA, S.L. se reserva el derecho de monitorizar y mantener trazas de las acciones llevadas a cabo por los usuarios en los sistemas informáticos, así como realizar acciones de mantenimiento sobre los equipos que puedan estar causando problemas de rendimiento o mal funcionamiento de los diferentes elementos que configuran la infraestructura de TI.

13. SUPERVISIÓN

13.1. Objetivo

Detectar las actividades de procesamiento de la información no autorizadas.

13.2. Registro de eventos

Para garantizar las operaciones de supervisión y auditoría de las actividades de los usuarios, la Organización activará, cuando considere necesario, las opciones de registro de eventos de los sistemas operativos de sus máquinas:

- Fechas y horas de inicio de sesión y cierre.
- Identidad y/o ubicación de usuario.
- Equipo desde el que se realiza el acceso y su dirección IP.
- Intentos de acceso con resultado error o rechazados.
- Registros de errores

13.3. Supervisión del uso del sistema

La supervisión de los registros de auditoría se realizará cada vez que se detecte un incidente de seguridad o cuando se reciba alguna alerta emitida de forma automática por los sistemas. El Responsable de Gestión será el encargado de la revisión de logs o registros, y deberá informar a la Dirección de cualquier incumplimiento o incidente que detecte para proceder a su solución.

13.4 protección de la información de los registros

Únicamente el Responsable de Gestión y la Dirección tendrán acceso a los registros o logs utilizados para auditoría, y será el único con privilegios suficientes para modificar o eliminar dichos registros.

13.5. Registros de administración y operación

Se seguirán las mismas consideraciones especificadas en los apartados 0 y 0 de este documento.

13.6. Registro de fallos

Los incidentes de seguridad detectados relacionados con el uso de información o sistemas de comunicación deberán registrarse conforme a lo establecido en la Política de Gestión de Incidentes de Seguridad de la Información. Los fallos o incidentes registrados deberán analizarse y tomar las acciones oportunas.

13.7. Sincronización del reloj

Con el fin de asegurar la exactitud de todos los registros y logs generados, todos los relojes de las máquinas estarán sincronizados con el servidor y este a su vez con un servidor NTP público.

POLÍTICA DE CONTROL DE ACCESO

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	25/03/2020	Emisión inicial
01	09/04/2021	Actualización formato

REVISADO Y APROBADO:

Firma:

Firma Juan Carlos Martínez Rodríguez
Fecha: 09/04/2021

Contenido

1. OBJETO

Establecer las reglas de aplicación para el control de acceso a la información.

2. ALCANCE

Esta Política es de aplicación a todas las áreas o sistemas con servicios de acceso lógico.

3. POLÍTICA DE CONTROL DE ACCESO

OPEMAT INGENIERÍA, S.L. ha establecido unas reglas sobre el acceso, tanto físico como lógico, de los usuarios o grupos de usuarios a los activos.

Dichas reglas serán comunicadas, tanto a los empleados como a terceros, de acuerdo a lo que necesite cada usuario para la realización de su trabajo.

Para el establecimiento de dichas reglas se han tenido en cuenta los siguientes criterios:

- → Requerimientos del negocio.
- → La evaluación de riesgos.
- → Requerimientos de seguridad de las aplicaciones de las que se hacen uso.
- → Identificación de los activos, y más concretamente, de la información a la que se puede acceder y su clasificación.
- → Inicio y final de la relación de los usuarios con la Organización.
- → Responsabilidades y funciones de los puestos definidos dentro de la Organización.
- → Relaciones contractuales con terceros.
- → Legislación aplicable (por ejemplo, LOPD).
- → Tipos de acceso disponibles.
- → Revisión periódica de los controles de acceso.
- → Autorización de las solicitudes de acceso.

En los siguientes puntos se desarrollan las reglas de control de acceso, que se complementan con el contenido de otras instrucciones de seguridad de la información.

4. GESTIÓN DE ACCESO DE USUARIOS

4.1. Objetivo

El objetivo de la gestión de accesos es garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

4.2. Inscripción de usuarios

Cuando se incorpore un nuevo empleado a la Organización se seguirá el siguiente procedimiento:

- Se creará un nuevo usuario en el sistema que lo identifique de forma única.
- Se asignará al usuario los permisos de acceso a recursos que le correspondan acorde a su puesto de trabajo y todos aquellos adicionales que estén especificados en su ficha de personal.
- Verificación del cumplimiento de las restricciones de seguridad, así como que el empleado tendrá acceso a la información y servicios necesarios para el desempeño de sus funciones.
- Cuando un usuario cambie de puesto de trabajo, será necesario revisar sus permisos de acceso y modificarlos si es necesario para adaptarlos a las nuevas responsabilidades y restricciones.

Cuando un empleado deje de prestar sus servicios a la Organización, se seguirá lo descrito en el procedimiento PR-02 Gestión de recursos humanos.

4.3. Gestión de privilegios

Las Fichas de Perfil puesto definen toda la información en cuanto a responsabilidades en materia de seguridad que se aplica a los empleados de la Organización, y las restricciones de acceso se asignarán en función de esa información.

4.4 manejo de contraseñas

Las directivas de seguridad en cuanto a gestión de las contraseñas a seguir por todos los empleados:

- Tras iniciar sesión por primera vez en el sistema el usuario deberá cambiar su contraseña.
- La longitud mínima de la contraseña debe ser de, al menos, 6 caracteres y debe contemplar normas seguras:
    - Letras
    - Números
    - Caracteres especiales

- Queda terminantemente prohibido el envío de contraseñas a través de mensajes de correo electrónico, o medios de comunicación no seguros, sin permiso de la Dirección.
- Cuando se instale nuevo software, se cambiarán las contraseñas predeterminadas del fabricante.
- Cuándo se realice un cambio de contraseña no se podrá introducir ninguna igual a las últimas 2 anteriores.
- La contraseña debe cambiarse al menos anualmente.
- Evitar guardar la contraseña a no ser que pueda ser almacenada de forma segura y que el método de almacenamiento haya sido probado.
- Cambiar la información secreta de autenticación siempre que haya indicios de su posible compromiso.

4.5. Revisión de derechos de acceso

Los derechos de acceso de los usuarios se revisarán de acuerdo a las Fichas de Perfil de Puesto y a lo especificado en las Fichas de Personal, cuando se produzca una modificación en el puesto de trabajo de un usuario: ascenso, cambio de puesto, etc.

También se revisarán los permisos de acceso en las siguientes situaciones:

- Cuando se produzcan nuevas incorporaciones de activos, modificaciones en la clasificación de la información, etc.
- Periódicamente (cada año) para comprobar que cada usuario sigue teniendo únicamente los permisos de acceso que le corresponden, verificando que no se hayan obtenido privilegios no autorizados.
- Cuando un empleado se traslade de puesto de trabajo dentro de la misma organización.

5. RESPONSABILIDAD DEL USUARIO

5.1. Objetivo

Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.

5.2. Uso de claves secretas

Además de las consideraciones establecidas en el apartado 0 Manejo de contraseñas, los usuarios cumplirán las siguientes obligaciones en el uso de sus contraseñas:

- No almacenar nunca contraseñas en papel o dispositivos electrónicos si no se han protegido de forma adecuada.
- Solicitar el cambio de la contraseña de acceso cuando exista el menor indicio de un posible peligro.
- No compartir las claves secretas individuales.

- Asegurar la confidencialidad de sus contraseñas, y de cualquier contraseña que conozca debido a su puesto o responsabilidad.
- No usar la misma clave personal para propósitos comerciales y no-comerciales.
- Cuando necesiten utilizar diferentes contraseñas para acceso a diferentes servicios se recomienda utilizar un gestor de contraseñas.
- Se evitará siempre la utilización de los recordatorios de contraseñas. Queda terminantemente prohibido su uso en sitios web.
- Para facilitar la generación de contraseñas seguras se podrá utilizar la siguiente aplicación web: http://password.es

5.3. Equipo del usuario desatendido

Todos los usuarios deberán estar al tanto de los requisitos de seguridad y deberán tener en cuenta las siguientes medidas cuando dejen su equipo desatendido:

- Los protectores de pantalla de los equipos de los usuarios deberán activarse automáticamente tras 10 minutos de inactividad, bloqueando a su vez el equipo. En su reanudación, será necesaria introducir nuevamente el usuario y contraseña.
- Los protectores de pantalla seleccionados deben ocultar el contenido de la pantalla.
- Los equipos se bloquearán automáticamente tras 30 minutos de inactividad.
- Cuando un usuario abandone su puesto por un periodo 10 minutos deberá bloquear el equipo.

5.4. Política de escritorio y pantalla limpios

Los empleados seguirán las pautas descritas en la Política de Clasificación de la información en cuanto a la manipulación de los distintos tipos de información (confidencial, de uso interno, pública) independientemente del formato en el que se encuentre.

Los empleados deberán conservar la pantalla del ordenador libre de accesos directos a información, servicios o medios de procesamiento que puedan suponer un riesgo para la seguridad de la información. En todo caso, no se podrán mantener accesos directos a documentos, archivos, directorios, etc. en la pantalla del ordenador que deban estar sujetos a restricciones de acceso (información confidencial o de proyectos, directorios de código fuente, etc.).

Las mesas de trabajo de los empleados deberán estar limpias y ordenadas, y en ningún caso deberán quedar documentos o información confidencial sobre las mismas. Toda la documentación o información confidencial que temporalmente esté manejando un empleado, deberá devolverse a su lugar de almacenamiento en cuanto se termine su uso, o custodiarla bajo llave en la cajonera de la mesa en los periodos de abandono temporal de puesto de trabajo.

6. CONTROL DE ACCESO A REDES

6.1. Objetivo

Impedir el acceso no autorizado a los servicios de red.

6.2. Política sobre el uso de los servicios de la red

Los controles de acceso a los servicios de la red se establecerán teniendo siempre en cuenta las **Fichas de perfil de puesto** en las que se recogen las responsabilidades en materia de seguridad y si algún empleado cuenta con permisos de acceso especiales.

6.3. Autenticación del usuario para las conexiones externas

Están permitidas las conexiones remotas de usuarios a los servidores de la Organización, realizadas mediante certificados de conexión segura y contraseña de usuario. Además, la conexión remota debe estar aprobada por Dirección.

Las conexiones remotas que se realicen desde la organización contra equipos de terceros (clientes o proveedores) se realizaran de acuerdo a las pautas y normas de seguridad establecidas por el tercero.

6.4 identificación del equipo en las redes

En la red interna, todos los equipos están identificados a través de su dirección IP, además de un nombre de equipo único.

6.5. Segregación de redes

Dadas las dimensiones y necesidades de la Organización no se ha considerado necesario la segregación de redes.

6.6 control de conexión a la red

Las restricciones de acceso a los diferentes servicios de la red se establecerán tomando como punto de partida las responsabilidades en materia de seguridad y funciones de los empleados especificadas en las Fichas de perfil de puesto.

La conexión a la red interna no estará restringida en función de horarios, y todos los usuarios tendrán acceso a los servicios que necesiten para el correcto desempeño de su trabajo.

6.7. Control de routing de la red

Dado que en la Organización no hay redes segregadas, ni la red se extiende más allá de las oficinas de la empresa, no se considera necesario establecer ningún control de enrutamiento.

7. CONTROL DE ACCESO AL SISTEMA OPERATIVO

7.1. Objetivo

Impedir el acceso no autorizado al sistema operativo de los equipos de la Organización.

7.2. Procedimientos seguros de inicio de sesión

Los usuarios únicamente podrán iniciar sesión contra sus máquinas a través de un usuario y contraseña que deberán validarse contra el servidor de dominio de la organización.

7.3. Identificación y autenticación de usuario

El identificador de usuarios se generará como se especifica en el apartado 4.1. Inscripción de usuarios.

Las actividades de usuario no se realizarán desde cuentas con un alto nivel de privilegios.

7.4. Sistema de gestión de claves secretas

Se seguirán las directrices marcadas en los apartados 4.4. Manejo de contraseñas.

Impedir el acceso a usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.

Uso de claves secretas:

Cuando un usuario deba mantener un número elevado de cuentas de usuario con sus correspondientes claves de acceso se le recomienda utilizar un gestor de contraseñas.

7.5. Uso de las utilidades con privilegios del sistema

Por otro lado, cualquier otro usuario deberá solicitar al Responsable del Sistema el uso de cualquier utilidad que pueda poner en peligro la seguridad del mismo (instalación/desinstalación de software, activación/desactivación de servicios, etc.)

7.6. Cierre de una sesión por inactividad

Aquellas aplicaciones o sistemas que lo permitan deberán tener configurado el cierre automático de sesión por inactividad. Cuando no sea posible los sistemas estarán salvaguardados por los controles e equipos desatendidos.

7.7. Limitación del tiempo de conexión

No se ha establecido ninguna limitación de tiempo de conexión a los sistemas o aplicaciones de la Organización.

8. CONTROL DE ACCESO A LA APLICACIÓN Y LA INFORMACIÓN

8.1. Objetivo

Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

8.2. Restricción del acceso a la información

El acceso a los sistemas de información solo estará permitido a los empleados y personal que disponga de la cuenta de usuario establecida por la Organización. Además según el tipo de usuario, tendrá acceso a las diferentes carpetas con la información necesaria para desarrollar los trabajos.

8.3. Aislar el sistema confidencial

Los sistemas confidenciales o que manejen información crítica deberán tener un ambiente de cómputo dedicado (aislado).

El servidor es el sistema más sensible dentro de la Organización, ya que contiene toda la información crítica del sistema. Por este motivo, se aplican las medidas de seguridad física explicadas en la Política de *Seguridad Física y Ambiental*, en su apartado Áreas seguras.

9. ORDENADORES PORTÁTILES Y TELETRABAJO

9.1. Objetivo

El objetivo de estos controles es asegurar la seguridad de la información cuando se utiliza medios de computación móviles y teletrabajo.

9.1. Computación y comunicaciones móviles

Las directivas de seguridad a este respecto que se aplicarán son las siguientes:

Equipos portátiles: Lo discos duros de los ordenadores portátiles que se utilicen fuera de las instalaciones estarán cifrados, o al menos dispondrán de una partición cifrada en al que se guardará la información confidencial. Además serán de aplicación los controles establecidos en la Política de Seguridad Física y Ambiental en su apartado relativo a la seguridad de los equipos fuera de las instalaciones, así como todos los recogidos en la Política de Gestión de comunicaciones y operaciones, relativos a la manipulación de la información y medios removibles.

9.3. Teletrabajo

El teletrabajo está permitido en la Organización. Se debe garantizar la seguridad de la información cuando se usen dispositivos móviles fuera de las instalaciones (se tendrá en cuenta todo lo especificado en el control 6.2.1 Política de dispositivos móviles). Para asegura que la información no esté comprometida, será obligatorio adoptar las siguientes medidas de seguridad cuando se trabaje en un entorno exterior desprotegido:

- Se deberán proteger físicamente los dispositivos móviles contra el robo, sobre todo en coches, habitaciones de hotel, centros de conferencias, cafeterías, etc. no se deberá dejar solo, o sin vigilar,

un equipo que contenga información importante, sensible o crítica; siempre que sea posible se dejará bajo llave o escondido.

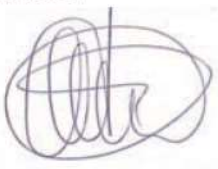
- Cuando la información sea altamente confidencial, se usarán técnicas de encriptación para evitar el acceso no autorizado o la divulgación de la información almacenada.
- Se deberán instalar y mantener al día antivirus y/u otros procedimientos contra software malicioso.
- Se deberá asegurar que la información sensible almacenada en estos dispositivos móviles tiene copia de seguridad recuperable en caso de pérdida o robo del dispositivo.
- Se deberá prestar un cuidado especial en proteger los dispositivos móviles que estén conectados a las redes. Solo se deberán hacer accesos remotos a la información de la empresa a través de redes públicas o de terceros, pasando por mecanismos de seguridad de control de accesos, y después de conseguir con éxito identificarse y autenticarse.
- Para el acceso a los equipos se tendrá en cuenta el Punto 6 de esta Política.

POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	18/03/2012	Emisión inicial
01	09/04/2021	Actualización de formato

REVISADO Y APROBADO:
Firma:



Firmado: Juan Carlos Martínez Rodríguez

Fecha: 09-04-2021

Contenido

1. OBJETO

Regular como debe llevarse a cabo la adquisición, desarrollo y mantenimiento de los sistemas de información de la Organización, garantizando la seguridad de la información y el correcto funcionamiento de los sistemas.

2. ALCANCE

Esta instrucción es de aplicación para toda adquisición, desarrollo o mantenimiento que se realice de los sistemas de información de la Organización.

3. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

3.1. Objetivo

Garantizar que la seguridad sea una parte integral de los sistemas de información (sistemas de operación, infraestructura, aplicaciones comerciales, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario, etc.)

3.2. Análisis y especificación de los requisitos de seguridad

Cuando sea necesaria la adquisición de nuevos sistemas para el tratamiento de la información de la organización se tendrán en cuenta las siguientes consideraciones:

- Cuando se implante un nuevo software se optará siempre o por software libre, o por software comercial legalmente comprado, teniendo en cuenta siempre los requisitos especificados en la Política de Control de acceso, en los apartados de Control de acceso a la red y Control de acceso a las aplicaciones y a la información.

- En la adquisición de nuevo software se valorará el nivel de integración que dicho software tenga con las aplicaciones que estén en uso en la organización.

- En cuanto al hardware se tendrá en cuenta el servicio post-venta y los requisitos de uso previsto para el hardware que se desee adquirir.

- Siempre se tendrá en cuenta a la hora de la adquisición, las medidas de seguridad que tanto el hardware como el software permitan aplicar.

3.3. Aseguramiento de los servicios de aplicación en las redes públicas

Este punto no resulta de aplicación para la Organización, ya que no se utilizan redes públicas para la transmisión de información sensible o para acceder a las aplicaciones.

4. TRATAMIENTO CORRECTO DE LAS APLICACIONES

4.1. Objetivo

Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones. Con tal objetivo se deberán diseñar controles apropiados en las aplicaciones para asegurar un procesamiento correcto, incluyendo la validación de los datos de entrada, el procesamiento interno y la validación de los datos de salida.

4.2. Validación de los datos de entrada

Cuando se adquieran, desarrollen o modifiquen aplicaciones o sistemas de información estos deberán ser sometidos a pruebas de validación de datos de entrada que comprueben entre otros: valores fuera de rango, caracteres inválidos, datos incompletos, campos obligatorios, etc.

4.3. Control del procesamiento interno

Cuando se adquieran, desarrollen o modifiquen aplicaciones o sistemas de procesamiento de información deberán someterse a pruebas de validación de procesamiento interno. Entre las pruebas realizadas podrá tenerse en cuenta: resultados correctos de las funciones de agregación, modificación o borrado de datos, capacidad para recuperarse tras errores de procesamiento, protección contra ataques utilizando desbordamiento de memoria, etc.

4.4 integridad de los mensajes

En aquellos casos en los que la aplicación de uso interno a desarrollar requiera del envío y recepción de mensajes, se implementarán los controles adecuados para asegurar la autenticidad e integridad de los mismos.

4.5. Validación de los datos de salida

Al igual que con los datos de entrada, cuando se adquieran, desarrollen o modifiquen aplicaciones o sistemas de procesamiento de información, deberán someterse a pruebas de validación de los datos de salida. Entre las pruebas realizadas podrán contemplarse las siguientes: los datos ofrecidos son correctos, la información mostrada es acorde a la precisión y exactitud requerida, los datos mostrados son los solicitados, etc.

5. CONTROLES CRIPTOGRÁFICOS

5.1. Objetivo

Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.

5.2. Política sobre el uso de controles criptográficos

Se tendrán en cuenta lo establecido en el documento **Gestión y clasificación de la información** (apartado Clasificación de la información) e **Gestión de comunicaciones y operaciones** (apartado Intercambio de información).

En cuanto al uso de controles criptográficos la organización establece las siguientes pautas:

- La empresa dispone de un certificado digital para la realización de trámites administrativos y legales. El responsable del uso y custodia de dicho certificado será la Dirección.
- Todos los medios físicos que salgan fuera de las instalaciones y que contengan información confidencial o de valor para la empresa deberán ir cifrados.
- El acceso desde el exterior se realizará mediante VPN cifradas o sistemas de usuario y contraseña que aseguren el acceso seguro desde el exterior.

5.3. Gestión de claves

Las claves utilizadas por las herramientas de cifrado deberán seguir las pautas establecidas en la **Política de Control de acceso** en su apartado Uso de contraseñas (apartados 4.4 y 5.2). Cuando los usuarios deban gestionar muchas contraseñas diferentes la organización aconseja utilizar algún software de repositorio.

6. SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

6.1. Objetivo

Garantizar la seguridad de los archivos del sistema, mediante el control de acceso a los mismos y al código fuente de los programas.

6.2. Control del software en explotación

Sólo el Responsable del Sistema y la Dirección tiene permiso para instalar software. En el caso de que un trabajador necesite instalar algún tipo de software, deberá comunicárselo previamente al Responsable del Sistema. Todo el software a utilizar será previamente analizado y aprobado.

Se prestará especial atención en el software de las plataformas que den servicio a clientes. Cualquier cambio en dichos sistemas se planificará y probará previamente en maquetas de implantación (máquinas virtuales) o a pequeña escala, para evitar el impacto en el servicio de los clientes.

Antes de realizar cualquier cambio en la configuración software de un equipo, deberán tomarse las medidas necesarias para poder hacer un "rollback" si fuera necesario. Los equipos de usuario, al ser fácilmente reemplazables, no requieren la planificación y pruebas.

6.3. Protección de los datos de prueba del sistema

Se evitará siempre la utilización de datos reales, especialmente información personal o confidencial real, en la realización de las pruebas de los sistemas.

En caso de ser necesaria la utilización de datos reales para pruebas de los sistemas, se trabajará con una copia de dichos datos, modificados en la medida de lo posible para evitar su reconocimiento. Una vez finalizadas las pruebas estos datos serán eliminados inmediatamente. Además, en el registro de las pruebas realizadas (si procede) se especificará qué base de datos se ha utilizado en su realización.

6.4. Control de acceso al código fuente de los programas

Para evitar modificaciones no controladas y cambios no autorizados en el código fuente de los programas, la Organización únicamente autoriza al personal del equipo de trabajo del proyecto correspondiente. Además el código fuente estará controlado y gestionado a través de una aplicación de control de versiones.

7. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

7.1. Objetivo

Mantener la seguridad del software y la información de las aplicaciones. Se deberían establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas. *Aunque actualmente no se realiza desarrollo de software en la organización, se deja especificado como se realizarían cada uno de los apartados que siguen, dentro de este punto 7, por si en el futuro les aplicase este apartado.*

7.2. Procedimiento de control de cambios

Al igual que los entornos de producción en la fase de desarrollo deberemos vigilar y controlar estrechamente desde la actualización de los navegadores a las actualizaciones de los sistemas operativos y la introducción de nuevas funcionalidades.

Siempre que sea posible los cambios se aplicarán sobre un entorno de preproducción y una vez verificados se pasarán al entorno real.

Antes de aplicar los cambios en el entorno de producción, y solo cuando sea imprescindible, se avisará a los clientes sobre los cambios a realizar. Por el contrario, cuando los cambios puedan realizarse sin que el cliente lo perciba, se procederá a su realización tomando siempre las medidas de seguridad oportunas que permitan volver al estado de partida en caso de que se produzca algún problema.

En la medida de lo posible, todos los cambios se aplicarán al entorno productivo en los momentos de mínima actividad.

7.3. Revisión técnica de las aplicaciones después de cambios en el sistema operativo

Una vez realizada una modificación en los sistemas operativos de los equipos, el Responsable de Gestión deberá comprobar que todas las aplicaciones críticas funcionan correctamente y no comprometen la seguridad de la información.

Para ello, las modificaciones y pruebas realizadas sobre la aplicación deberán ser realizadas tal y como se explica en el apartado **Gestión de los cambios** de la **Política de Gestión de comunicaciones y operaciones**, realizándolas sobre un equipo aislado o una máquina virtual. Así, las actualizaciones no generarán fallos de funcionamiento del sistema ni pondrá en peligro la integridad de la información y documentación manejada en los diferentes procedimientos.

Cuando se haya comprobado que los cambios introducidos no ponen en riesgo la seguridad del software y la información del sistema, se aplicarán en todos los equipos en los que estaba implantada anteriormente dicha aplicación.

7.4. Restricciones a los cambios en los paquetes de software

Antes de realizar cambios en los paquetes software empleados por la organización deberán analizarse los efectos de los mismos y seguir lo establecido en los apartados de **Control de Software en explotación** (punto 6.2) y **Procedimiento de control de cambios** (punto 7.2) de esta instrucción.

7.5. Principios de la ingeniería de sistemas seguros

Los principios de ingeniería seguros nos requieren documentar procedimientos sobre cómo implementar medidas de seguridad en las técnicas de desarrollo. La Organización no realiza desarrollos, por lo que no aplica este punto.

7.6. Entorno de desarrollo seguro

Los principios de ingeniería seguros nos requieren documentar procedimientos sobre cómo implementar medidas de seguridad en las técnicas de desarrollo. Como comentamos, la Organización no realiza desarrollos, por lo que este punto no resulta de aplicación.

7.7. Fugas/filtración de información

Para evitar los canales encubiertos que puedan generar filtraciones de información se tomarán en cuenta los procedimientos establecidos para la protección contra códigos maliciosos (ver **Política de Gestión de comunicaciones y operaciones**), así como para el control de acceso a la red (ver **Política de Controles de acceso**).

La Dirección podrá autorizar controles esporádicos de la actividad del personal y de los sistemas, siempre y cuando esté permitido por la legislación o regulaciones vigentes.

7.8. Externalización del desarrollo de software

El responsable de Gestión deberá verificar que el software entregado por terceros (si procede) cumple los requisitos establecidos para la adquisición (véase apartado Gestión de entrega de servicio de terceros de la **Política de Gestión de comunicaciones y operaciones**). Además deberán tenerse en cuenta los siguientes aspectos:

- Contratos de licencia, propiedad de código, derechos de propiedad intelectual, etc.
- Certificaciones de calidad y exactitud del trabajo desarrollado.
- Derechos de acceso para la realización de auditorías de calidad y seguridad.
- Prueba antes de la instalación para detectar códigos maliciosos y troyanos.

7.9. Pruebas funcionales de seguridad de sistemas

Los principios de ingeniería seguros nos requieren documentar procedimientos sobre cómo implementar medidas de seguridad en las técnicas de desarrollo. Al no realizar desarrollo, este punto no es de aplicación.

7.10. Pruebas de aceptación de sistemas

Se deberían establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones. Estas pruebas deberían incluir pruebas de los requisitos de seguridad de la información (Puntos 3.2 y 3.3 de esta Política) y de que se han aplicado prácticas de desarrollo seguro del sistema (Punto 7.1. de esta Política).

8. GESTIÓN DE VULNERABILIDADES TÉCNICAS

8.1. Objetivo

Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

8.2. Control de las vulnerabilidades técnicas

El Responsable del Sistema será la persona encargada de identificar las vulnerabilidades técnicas potenciales que pueden poner en riesgo la seguridad de los sistemas utilizados por la organización: a través de subscripciones a foros especializados y boletines, así como la revisión de los avisos emitidos por los fabricantes del software.

Antes de instalar cualquier parche de actualización de seguridad crítico, el Responsable del Sistema deberá informarse en páginas especializadas de las consecuencias que pueden derivar de dicha

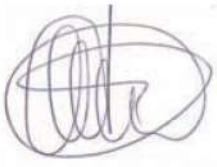
actualización. En todo caso, antes de llevar a cabo la actualización del servidor y de los sistemas críticos será necesario asegurar que dicha instalación no tendrá efectos adversos no deseados.

POLÍTICA DE GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	18/03/2012	Emisión inicial
01	09/04/2021	Actualización de formato

REVISADO Y APROBADO:
Firma:



Firmado: Juan Carlos Martínez Rodríguez

Fecha: 09-04-2021

Contenido

1. OBJETO

El objetivo de la presente instrucción es establecer cómo debe llevarse a cabo la gestión de incidentes de seguridad en la Organización.

2. ALCANCE

Esta instrucción es de aplicación para todos los incidentes en materia de seguridad de la información que se produzcan en la Organización.

3. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

3.1. Objetivo

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

3.2. Notificación de eventos y puntos débiles de seguridad de la información

Todos los empleados tienen la obligación de reportar cualquier evento en la seguridad de la información lo más rápidamente posible. Ningún empleado deberá probar la debilidad de seguridad sospechada debido al riesgo de causa de daños al sistema de información. También deberán anotar y notificar cualquier punto débil que observen o sospechen que exista.

Para ello, se informará mediante correo electrónico al Responsable del Sistema sobre su existencia. Adicionalmente se incluirá detalle de los activos afectados por la incidencia, además de una descripción detallada de la misma. Una vez el Responsable del Sistema revisa la incidencia será el encargado de su registro y de establecer las acciones necesarias.

A continuación, se indican algunos ejemplos de incidentes de seguridad de la información:

- Pérdida del servicio, equipos o medios.
- Mal funcionamiento o sobrecarga de los sistemas.
- Errores humanos.
- Incumplimiento de las políticas o estándares de seguridad.
- Vulneraciones de los acuerdos de seguridad física.
- Cambios del sistema no controlados.

- Mal funcionamiento del software o del hardware.
- Violaciones de acceso.
- Etc.

El mal funcionamiento o cualquier otra conducta anómala del sistema pueden ser un indicador de un ataque a la seguridad o una verdadera violación de la seguridad, por lo tanto, siempre deberá notificarse como un evento en la seguridad de la información.

Para el registro de las incidencias de seguridad, el Responsable del Sistema empleará el formato Registro de incidencias de seguridad.

4. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS

4.1. Objetivo

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información, para lo cual se establecerán las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información.

4.2. Responsabilidades y procedimientos. Evaluación y decisión sobre eventos de SI. Respuesta a incidentes de SI

Todos los empleados tienen obligación de reportar los eventos y vulnerabilidades detectados en la seguridad de la información, para lo cual se utilizará el procedimiento especificado en el apartado ¡Error! No se encuentra el origen de la referencia.¡Error! No se encuentra el origen de la referencia..

El Responsable del Sistema será el encargado de registrar, evaluar e iniciar las acciones correctivas y preventivas necesarias, así como las causas del incidente registrado.

Las incidencias de seguridad se gestionarán en la hoja de Registro de Incidentes de Seguridad. De todos los incidentes de seguridad de la información que se produzcan se dejará constancia de la siguiente información:

- Descripción de la incidencia
- Quién ha detectado la incidencia
- Fecha en la que se ha detectado o se ha recibido la notificación de la incidencia
- Activos afectados
- Impacto de la incidencia:

  - Bajo: la incidencia no provoca la parada ni la degradación de ningún servicio interno ni externo.
  - Medio: la incidencia provoca la degradación de algún proceso o servicio.
  - Alto: la incidencia provoca la parada de algún proceso o servicio.
- Acción planificada para solventar la incidencia
- Responsable de ejecución de la/s acciones
- Estado en el que se encuentra la incidencia:
  - Abierta: toda incidencia recién registrada.
  - En proceso: cuando se ha empezado a realizar las acciones correspondientes a la incidencia.
  - Cerrada: una vez que se han cerrado y verificado las acciones asociadas a la incidencia.
- Fecha de resolución/cierre de la incidencia
- Observaciones

Los incidentes de seguridad que se hayan repetido tres o más veces en los últimos doce meses, o que supongan un incumplimiento de los requisitos de la norma UNE-ISO/IEC 27001, deberán ser considerados como una No Conformidad. En estos casos, el Responsable del Sistema indicará, en el Registro de Incidencias de Seguridad, que el incidente pasa a convertirse en no conformidad, incluyendo el código identificativo de la misma.

4.3. Aprendizaje de los incidentes de seguridad de la información

Anualmente, el Responsable del Sistema realizará un análisis sobre los incidentes reportados en materia de Seguridad de la Información, coincidiendo con la Revisión del Sistema, en el que la Dirección y el Responsable del Sistema dictarán, si procede, las medidas correctivas que sean oportunas, incluyendo, si es preciso, la publicación a nivel interno de actitudes o acciones a tener en cuenta ante posibles futuros incidentes.

4.4. Recopilación de evidencias

Cuando un incidente de seguridad requiera una acción legal (tanto civil como criminal) contra su responsable/s, es necesario recolectar y mantener evidencias que se pueden presentar en el momento de aplicar una acción disciplinaria.

Como evidencias se utilizarán (siempre al amparo de la legislación vigente):

- Los registros y monitorización de las actividades del empleado/s sobre los sistemas de información en el momento de producirse el incidente.
- El equipo o dispositivos de almacenamiento del empleado si las características del incidente así lo requieren (detección de información fraudulenta en el equipo, detección de filtraciones de información confidencial, etc.).
- Otras evidencias aplicables.

Todas las evidencias recolectadas serán almacenadas de forma segura, realizando copias de seguridad de la misma. El responsable de su almacenamiento será la Dirección de la Organización, que se asegurará de que ninguna persona no autorizada accede a dichas evidencias.

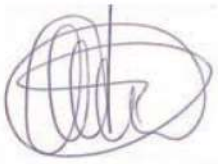
En el caso de evidencias contenidas en papel, el original debería ser almacenado de forma segura, creando un registro con los datos de la/s persona/s que han descubierto el documento, la fecha y hora del hallazgo, y el lugar donde se encontraba.

POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	18/03/2012	Emisión inicial
01	09/04/2021	Actualización de formato

REVISADO Y APROBADO:
Firma:



Firmado: Juan Carlos Martínez Rodríguez

Fecha: 09-04-2021

Contenido

1. OBJETO

El objetivo de la presente es el de establecer un marco de referencia para la implantación y gestión de la continuidad de negocio.

2. ALCANCE

Este documento es de aplicación a todos los aspectos relacionados con la planificación, mantenimiento, prueba y reevaluación de los planes de continuidad de negocio.

3. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

3.1. Objetivo

Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos críticos de los efectos de fallos o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación. Esta Política debe analizarse conjuntamente con el PR-27 Plan de Continuidad del Negocio.

3.2. Incluir la seguridad de la información en el proceso de gestión de la continuidad de negocio

A partir de la evaluación de riesgos de la Dirección, con la colaboración del Responsable del Sistema, establecerá un Plan de Continuidad de Negocio. Se entenderá por Contingencia aquellas situaciones que puedan poner en peligro la continuidad del negocio de la Organización.

Para identificar las posibles situaciones de contingencia deberán tener en cuenta los siguientes aspectos:

- La evaluación de riesgos.
- Los procesos comerciales críticos de la organización.
- El posible impacto de la interrupción de los procesos comerciales por incidentes de seguridad.
- Seguros que cubran los riesgos sobre la continuidad de negocio.
- Controles preventivos adicionales.
- Recursos financieros, organizacionales y técnicos suficientes para los requerimientos de seguridad de la información identificados.
- Garantizar la seguridad del personal y la protección de los medios de procesamiento de la información y la propiedad organizacional.

- Las instrucciones documentadas sobre la Seguridad de la Información.
- Pruebas y actualizaciones regulares de los planes.

3.3. Continuidad del negocio y evaluación de riesgos

Para identificar los eventos que pueden causar las interrupciones en los procesos comerciales se tendrán en cuenta los siguientes aspectos: fallos en los equipos, errores humanos, robo, fuego, desastres naturales o actos intencionados. Todos ellos se habrán incluido en la evaluación de riesgos de acuerdo a lo establecido en el procedimiento de Evaluación de Riesgos.

Sobre dicha evaluación, se identificarán las posibles situaciones que puedan ocasionar la interrupción de los procesos críticos y por tanto comprometer la continuidad del negocio. Partiendo de dicha identificación, se establecerá un Plan de Continuidad aprobado por la Dirección.

3.4. Desarrollo e implementación de planes de continuidad incluyendo seguridad de la información

La Organización definirá un Plan de Continuidad de Negocio en el que:

- Se establecerá el marco temporal tras el que debe activarse el plan de continuidad.
- Se determinan las situaciones de contingencia críticas y los planes de recuperación de cada una de ellas.
- Se identifican las tareas a realizar y los responsables de cada tarea para poner en marcha los planes de continuidad.
- Se establecen los tiempos de recuperación ante desastres.
- Se determinan los recursos necesarios para poner en marcha la continuidad de negocio en función de cada escenario de desastre.

Esta información se comunicará e informará a todos los involucrados en los diferentes escenarios del Plan de Continuidad de Negocio.

3.5. Marco de referencia para la planificación de la continuidad de negocio

El Plan de Continuidad de Negocio se desarrollará de acuerdo a lo recogido en el punto anterior. Además, se tendrá en cuenta que si éste afecta a cualquier otro procedimiento establecido en la empresa, éste deberá ser revisado para su adecuación a lo contenido en dicho Plan.

Por otro lado, el Plan de Continuidad de Negocio será tenido en cuenta dentro de la Revisión por la Dirección para su adecuación a los cambios que se produzcan en la organización.

Los Planes de Continuidad de Negocio deben ser comunicados y conocidos por los responsables de su aplicación, y en el caso de terceros, fundamentalmente proveedores de servicios, serán tenidos en cuenta en los acuerdos contractuales.

3.6. Prueba, mantenimiento y reevaluación de los planes de continuidad de negocio

La Organización establecerá un plan de Pruebas en el que se defina cuándo, cómo y quiénes serán los responsables de realizar las pruebas del Plan de Continuidad de Negocio.

Los escenarios de desastre definidos en el Plan de Continuidad de Negocio deberán ser probados a lo largo del periodo establecido en el Plan de Pruebas.

Cuando se disponga de un entorno real apropiado, se realizará una simulación de las actuaciones previstas, prueba de la recuperación de los activos afectados (datos, ordenadores, locales, etc.) y una simulación completa del incidente que podría motivar la puesta en marcha del Plan de Continuidad de Negocio.

Cuando las pruebas no puedan llevarse a cabo sobre un entorno real se procederá a simular la secuencia de actuaciones a realizar para tratar de detectar cualquier inconveniente o divergencia con respecto al plan establecido.

En el caso de que participe algún proveedor en las actuaciones previstas según los planes de contingencia, también se evaluarán los compromisos recogidos en contrato.

Las pruebas realizadas se registrarán indicando los puntos comprobados, las lecciones aprendidas, las debilidades detectadas y los cambios necesarios.

Tras la realización de las pruebas podrá ser necesario modificar el Plan de Continuidad para ajustar los cambios detectados. También será necesario revisar el plan cuándo:

- Se realicen cambios sobre los activos de la Organización.
- Se produzcan actualizaciones relevantes en los sistemas.
- Se produzcan cambios en personal, las instalaciones, los servicios prestados, proveedores o colaboradores, etc.

3.7. Redundancias. Disponibilidad de los recursos de tratamiento de la información

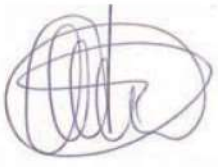
Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad. En este caso, y basándonos en las características de la Organización, los recursos de tratamiento de la información se consideran suficientes, si bien, se estudiará la necesidad de incorporar nuevos recursos en caso de que se den cambios en la misma.

POLÍTICA DE CUMPLIMIENTO DE REQUISITOS LEGALES Y POLÍTICAS

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	18/03/2012	Emisión inicial
01	09/04/2021	Actualización de formato

REVISADO Y APROBADO:
Firma:



Firmado: Juan Carlos Martínez Rodríguez

Fecha: 09-04-2021

Contenido

1. OBJETO

Evitar violaciones de cualquier ley u obligación estatutaria, regulación o contractual, y de cualquier requisito de seguridad.

2. ALCANCE

Esta instrucción es de aplicación a todos los procedimientos de transferencia y uso de información que maneja la Organización.

3. CUMPLIMIENTO DE REQUISITOS LEGALES

3.1. Objetivo

Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.

3.2. Identificación de la legislación aplicable

El convenio colectivo aplicable, establece el marco legislativo aplicable a las actividades de la empresa. Entre otras, específicamente se deberá prestar atención al cumplimiento de las siguientes leyes o normativas:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD). Esta norma introduce unos requisitos sobre la defensa de la intimidad y privacidad de los ciudadanos y consumidores, a los que reconoce un conjunto de derechos.

- Reglamento (UE) 2016/679 Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta norma introduce unos requisitos sobre la defensa de la intimidad y privacidad de los ciudadanos y consumidores, a los que reconoce un conjunto de derechos.

- Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE). La finalidad de esta Ley es regular el funcionamiento de prestadores de servicios de la Sociedad de la Información, empresas que realizan comercio electrónico, y aquellas que hacen publicidad por vía electrónica, como correo electrónico o SMS.

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. El objeto de la Ley es la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas.

- Ley 59/2003 de 19 de diciembre, de Firma Electrónica, que regula el uso de la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

3.3. Derechos de propiedad intelectual (dpi)

En general, se prohíbe el uso, copia o archivo de cualquier documento o software sometido a derechos de propiedad intelectual cualquiera que sea su soporte, físico o electrónico, sin la autorización de la Dirección.

La adquisición o copia de cualquier documento o instalación de software sometido a derechos de propiedad intelectual deberán ser autorizados por el Responsable del Sistema y/o la Dirección, y se realizará a través de fuentes conocidas.

En caso de que se adquiera software libre o cualquier documento no sometido a derechos de propiedad, el usuario deberá revisar previamente el acuerdo de licencia o copyright del documento en cuestión.

Por otra parte, se prohíbe la distribución o cesión de cualquier software o información propiedad de la Organización, si dicha distribución no ha sido autorizada por el Responsable del Sistema y/o la Dirección.

En caso de que se incumpla los derechos de propiedad, el poseedor del documento o software que ha causado dicho incumplimiento será el responsable del mismo, al que se le aplicará el régimen sancionador establecido por la Organización.

Queda permitido en la organización hacer copias de respaldo del software legalmente adquirido.

3.4. Protección de los registros de la organización

Todos los registros de la Organización se controlan de acuerdo a lo recogido en los procedimientos PR-01 Control de la documentación y los registros.

En general, se deberán preservar de agentes externos que puedan ocasionar su pérdida. En aquellos casos que así se establezca se realizarán copias de seguridad para poder respaldarlos en caso de pérdida o deterioro.

Además, se tendrá en cuenta lo especificado en la Política de Gestión y clasificación de la información.

3.5. Protección de los datos y privacidad de la información personal

Toda la información que contenga datos de carácter personal se clasificará como información crítica, y se tendrá en cuenta la reglamentación vigente en materia de Protección de Datos. También se tendrá en cuenta lo expuesto en el procedimiento de Gestión de Recursos Humanos para el tratamiento de la información del personal. Para este tema, se cuenta con colaboración externa para el cumplimiento de la legislación y reglamentación aplicables.

3.6. Prevención del mal uso de las instalaciones de procesamiento de información

En cuanto a las instalaciones de procesamiento de información, la Dirección aprueba su uso de acuerdo a lo expuesto en la Política de Gestión y clasificación de la información, en cuanto a la responsabilidad de los activos, y en la Política de Control de Acceso.

A todos los usuarios se les comunicará su acceso permitido y se les informará de la monitorización que se realiza sobre sus actividades, con el fin de detectar usos no autorizados, en base a los cuales se podrán adoptar medidas disciplinarias.

Se actuará de forma análoga con terceros que puedan tener acceso a nuestras instalaciones de procesamiento, dejando constancia en los acuerdos contractuales.

3.7. Regulación de los controles criptográficos

En caso de utilizar mecanismos de cifrado deben tenerse en cuentas las normativas sobre uso de controles criptográficos vigentes. En España deberemos tener en cuenta las siguientes leyes:

- La Ley General de Telecomunicaciones
- Ley de Firma electrónica

Además, debemos tener en cuenta el reglamento RGPD donde se establece la obligatoriedad de cifrar los datos de carácter personal para los datos clasificados como:

- De origen étnico o racial
- Opiniones políticas
- Convicciones religiosas o filosóficas
- Afiliación sindical
- Datos de salud y vidas sexuales
- Datos biométricos
- Uso de datos a gran escala afectados por sistemas de acceso publico

En el caso de que la Organización se vea obligada a cifrar datos según lo expuesto anteriormente, se deberán dedicar los recursos necesarios para cumplir con estos requisitos.

4. CUMPLIMIENTO DE POLÍTICAS Y NORMAS DE SEGURIDAD

4.1. Objetivo

Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la Organización.

4.2. Cumplimiento de las políticas y normas de seguridad

La Dirección, analizará el cumplimiento de los controles y normas establecidas en cuanto a seguridad, con el fin de mejorar la eficacia del sistema.

Al menos una vez al año la Dirección, junto al Responsable del Sistema, procederán a revisar el sistema de acuerdo a lo recogido en el procedimiento de Auditoría Interna.

En función de los incumplimientos detectados y las necesidades de mejora identificadas, procederá a determinar las causas del incumplimiento, establecer Acciones correctiva, y revisar el resultado de aplicar estas acciones correctivas.

4.3. Comprobación del cumplimiento técnico

El Responsable de Gestión revisará anualmente la aplicación de los controles y el cumplimiento de las políticas y criterios establecidos en cuanto a seguridad, de acuerdo a lo recogido en el procedimiento Análisis de Riesgos.

En caso de que se hagan pruebas sobre penetración o sobre las vulnerabilidades con personal competente y autorizado por la Dirección, se tendrá en cuenta que dichas pruebas no comprometan la seguridad de los sistemas. Se guardará registro de dichas pruebas.

5. CONSIDERACIONES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

5.1. Objetivo

Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde este proceso.

5.2. Controles de auditoría de sistemas de información

Para el caso de la Auditoría Interna del Sistema se seguirá lo establecido en el procedimiento de Auditoría Interna, en donde se establece cómo llevar a cabo las auditorías del sistema y los requisitos que se deben cumplir.

En el caso de realización de Auditorías técnicas sobre los sistemas, deberemos tener en cuenta los siguientes aspectos:

- En el programa que desarrolle la auditoría se deben incluir los puntos a comprobar durante la misma, y este debería se comunicado por el Responsable del Sistema con la suficiente antelación a los miembros de la organización.
- Durante la auditoría, el auditor o el equipo auditor, podrá acceder a la lectura de los registros y documentos del sistema, pero deberá cumplir con las normas de confidencialidad y seguridad

establecidas. Con el fin de minimizar el riesgo, los accesos a registros y archivos de la Organización deberían realizarse en modo de sólo lectura.

- Deberán estar disponibles los recursos necesarios para realizar las comprobaciones, incluidas las herramientas para comprobar la eficacia de los controles.
- Se dispondrá de las herramientas para procesar los resultados de la auditoría, cumpliendo en todo momento las normas de seguridad establecidas.

5.3. Protección de las herramientas de auditoría de sistemas de información

Todos los registros y herramientas para realizar comprobaciones y auditorías (logs, listas de control de acceso, registros de actividad, etc.) deberán estar bajo el control del Responsable del Sistema, así como los registros resultantes de las mismas. Dichos elementos estarán a disposición de la Dirección para cualquier comprobación o análisis que desee realizar.

En el caso de que participen terceros en la auditoría, el Responsable del Sistema los acompañará en todo momento, recabando la colaboración del resto de personal en caso necesario.

Además, se tendrá en cuenta lo expuesto en la Política de Controles de Acceso.

5.4. Cumplimiento de las políticas y las normas de seguridad

Este control pone como requisito la necesidad de que los responsables de cada área deben revisar que los procedimientos de la organización sean aplicados de acuerdo a los requisitos definidos. Para ello los responsables deberán:

- Determinar la forma de revisar cómo se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y en otras regulaciones aplicables.
- Tener en cuenta la implementación de sistemas de medición automática y herramientas de informes

Cuando se identifican incumplimientos se deberá:

- Identificar las causas
- Evaluar la necesidad de tomar medidas
- Implementar las acciones correctivas apropiadas;
- Revisar la eficacia de las acciones correctivas
- Identificar las deficiencias y debilidades del sistema

Para mantener registros documentados de esto, se procederá como en el Procedimiento de GESTIÓN DE NC Y AACC.

5.5. Revisión del cumplimiento técnico

Se comprobará periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información con las que cuenta la organización.

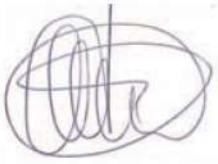
Para la evaluación de los sistemas de información debe revisarse periódicamente si están configurados correctamente de acuerdo a las reglas y políticas definidas. El objetivo es: Identificar fallos en las actualizaciones de los sistemas y Establecer medidas correctivas antes de que estos fallos puedan suponer una amenaza real para el sistema.

POLÍTICA DE GESTIÓN DE COPIAS DE SEGURIDAD

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	18/03/2012	Emisión inicial
01	09/04/2021	Actualización de formato

REVISADO Y APROBADO:
Firma:



Firmado: Juan Carlos Martínez Rodríguez

Fecha: 09-04-2021

Contenido

1. OBJETO

El objeto de esta Política es definir el sistema de actuación establecido por OPEAMT INGENIERÍA, S.L. para la realización de las copias de seguridad necesarias para salvaguardar la información afectada por este sistema.

Se aplica a la información automatizada incluida en el sistema de información de esta Organización.

2. ALCANCE

Esta Política es de aplicación a la realización de las copias de seguridad que realiza la Organización.

3. REALIZACIÓN DE LAS COPIAS DE SEGURIDAD

De forma automática, y a través del programador del software de backup de Synology, se lanza el proceso de copia con periodicidad semanal y mensual, conservando ambas copias indistintamente sobre el NAS remoto situado en una ubicación distinta de la oficina. Esta copia mantiene un reflejo idéntico al original. Además, localmente y de forma semanal (en la madrugada del domingo) se realiza copia sobre disco USB nombrado Seguridad, esta está encriptada y mantiene versionado de archivos, que por el momento al haber espacio suficiente no ha sido delimitado a un número concreto.

Se tiene otro disco donde se almacenan imágenes que se realizarán a petición de los usuarios a través del programa de creación de imágenes de disco VEEM. Donde cada usuario podrá lanzar la creación de una imagen de su puesto si así lo considera necesario.

Además, en el NAS está habilitada la papelera de reciclaje en Red que recoge todos los archivos eliminados conservando éstos hasta que se eliminen manualmente de forma definitiva y el versionado de archivos hasta 4 versiones, que mantiene las 4 últimas modificaciones de cada archivo.

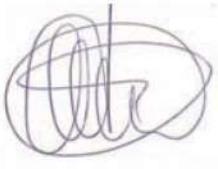
No obstante, lo expuesto anteriormente, se realizan copias de seguridad adicionales previamente a la realización de cualquier intervención técnica en los recursos informáticos, como la instalación o sustitución de hardware, reparaciones, así como cualquier otra intervención o incidencia sobre los recursos y sistemas informáticos que pueda afectar a la integridad de los datos.

POLÍTICA DE GESTIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

ESTADO DE REVISIONES

REVISIÓN	FECHA	MODIFICACIÓN
00	18/03/2012	Emisión inicial
01	09/04/2021	Actualización de formato

REVISADO Y APROBADO:
Firma:



Firmado: Juan Carlos Martínez Rodríguez

Fecha: 09-04-2021

Contenido

1. OBJETO

La información debe clasificarse para indicar la necesidad y prioridades para asegurar un nivel de protección adecuado.

2. ALCANCE

Este procedimiento es de aplicación a toda la información que maneja la Organización.

3. DIRECTRICES DE CLASIFICACIÓN

La información debe clasificarse en función de su valor, requisitos legales, sensibilidad y criticidad para la Organización. OPEMAT INGERNIERÍA, S.L. clasifica la información diferenciándola en las siguientes categorías:

Clase de Información	Característica	Disponibilidad	Difusión
Pública	Información comercial y publicitaria de la empresa: • Información de página web.	Todos	A todo el personal y a particulares
De uso interno	Datos de difusión sin restricción dentro de la organización o departamento correspondiente, por ejemplo: • Organigramas • Políticas y estándares • Información sobre procesos. • Metodologías utilizadas • Programas y utilidades • Software • Ofertas a clientes • Presupuestos • Facturas • Procedimientos operativos	Los empleados del departamento correspondiente de OPEMAT INGENIERÍA, S.L.	A todo el personal. No debe darse a conocer a los particulares (excepto a clientes afectados por tal información).
Confidencial	Aquella información con cierto grado de protección, ya que su conocimiento y divulgación por parte de personas no autorizadas puede causar daños graves a la Organización, clientes y/o terceros: • Información de trabajos con clientes	Difusión no autorizada. Los empleados del departamento correspondiente de OPEMAT INGENIERÍA, S.L.	A todo el personal involucrado. No debe darse a conocer a particulares

Crítica	Aquella información que requiere el máximo grado de protección, ya que su conocimiento y divulgación por parte de personas no autorizadas puede causar daños graves a la Organización, clientes y/o terceros: • Datos de clientes o proveedores • Información de trabajos de clientes a los que sólo puede acceder cierto personal en concreto • Información de configuración de la red • Resguardos o copias de seguridad • Información sobre seguridad informática (contraseñas de acceso, claves, etc). • Plan estratégico de la empresa • Contrato • Acuerdos de confidencialidad	Difusión no autorizada. Con acceso restringido a aquel personal cuyo ámbito específico de trabajo necesite el uso de alguna de esta información y posea autorización de la Dirección.	No debe darse a conocer a particulares ni a personal que no tenga permisos de Dirección.

Clase de Información	Periodo de Conservación
Pública	Permanente, siempre que esté actualizada.
De uso interno	Dependiendo de la información. Ver tiempos de conservación en registro RE-01-01 Documentación vigente del sistema. Toda aquella información que no esté contenida en este registro se almacenará hasta que deje de tener utilidad para la organización.
Confidencial y crítica	Dependiendo de la información. Ver tiempos de conservación en registros RE-01-01 Documentación vigente del sistema. Toda aquella información que no esté contenida en este registro se almacenará hasta que deje de tener utilidad para la organización.

4. ETIQUETADO Y MANIPULADO DE LA INFORMACIÓN

4.1. Información confidencial y crítica

Almacenamiento. Será almacenada por su propietario en el sistema de ficheros o la herramienta interna adecuada, según corresponda.

Si el documento llega en formato papel, se almacena en su carpeta correspondiente, teniendo en cuenta las siguientes pautas:

- La documentación CRÍTICA se almacenará en armarios o cajoneras bajo llave.
- La documentación CONFIDENCIAL Y CRÍTICA estará archivada en AZ o carpetas etiquetados con pegatinas.

Copia. La copia de este tipo de información sólo deberá realizarla Dirección o el personal autorizado a su manejo.

Destrucción. En caso de información impresa, para su destrucción se utilizará *la destructora de papel* existente. En caso de información en formato electrónico, se utilizarán herramientas de borrado seguro o la destrucción completa del soporte en el que se encuentre (CD, DVD, llave USB, etc.).

Difusión. Se tratará de asegurar en la medida de lo posible la transmisión de esta información:

- → A través de correo electrónico, se solicitará siempre acuse de recibo/lectura.
- → A través de soporte físico, se la información viajará cifrada o protegida por contraseña.
- → A través de correo ordinario, nunca se utilizará correo ordinario para el envío de información confidencial, sino que se utilizarán alternativas seguras: correo certificado, mensajería, etc.
- → Transmisión oral:
  - Se tomarán las medidas de seguridad oportunas para garantizar que sólo el interlocutor recibe la información (reuniones a puerta cerrada, verificación de la identidad del interlocutor de la línea telefónica, etc.).
  - No se dejarán mensajes con información confidencial en contestadores automáticos o buzón de voz.

4.2. Información de uso interno

Almacenamiento. El responsable de su almacenamiento será su propietario. Este tipo de información estará accesible al personal de la organización ya que es necesaria para llevar a cabo la actividad diaria de la empresa.

Copia. No es necesaria ninguna autorización, no obstante, será su propietario el encargado de realizar su copia y distribución.

Destrucción. Para su destrucción se procederá igual que en el caso de la información confidencial.

Difusión:

- → A través de correo electrónico, será el responsable del envío quien deberá considerar la necesidad o no de utilizar aviso de confidencialidad.
- → A través de correo ordinario, se podrá utilizar este medio para su envío.

4.3. Información pública

No existen restricciones respecto a su almacenamiento, copia, destrucción ni transmisión.