Política de seguridad de la información

Título	Política de seguridad de la información
Objeto	Establecer la política de seguridad de la información de Uriach
Autor	Oficina de Ciberseguridad
Aprobado por	Comité de Riesgos y Compliance

1. INTRODUCCIÓN

El objetivo de esta política es proporcionar orientación y apoyo para la gestión de la seguridad de la información, de conformidad con los requisitos empresariales y la normativa aplicable. Por ello, el marco de referencia de esta política es la norma ISO 27001, complementada por la norma ISO 27002.

Esta política contiene una descripción de los principales elementos humanos, organizativos, tecnológicos y documentales que Uriach aplica para proteger la información y, en especial, los datos de carácter personal, a fin de prevenir incidentes de seguridad que los pongan en riesgo.

En todos los niveles de la organización se velará por la aplicación real y efectiva de las medidas recogidas en esta política, de forma que este sistema de autorregulación consiga la eliminación de conductas que puedan poner en riesgo la seguridad de los activos de información y datos de carácter personal tratados por Uriach.

Esta política se adaptará a los cambios tecnológicos y legislativos que puedan producirse en el futuro, así como a los cambios organizativos que puedan surgir en Uriach.

2. ÁMBITO DE APLICACIÓN

En el ámbito de aplicación de este Protocolo, podemos distinguir:

a) El **ámbito corporativo.** El presente Protocolo es de aplicación a todas las empresas pertenecientes a Uriach, así como a las filiales y empresas participadas sobre las que Uriach tenga control efectivo u ostente un cargo de miembro en los órganos de dirección.
b) El **ámbito personal.** El presente Protocolo es aplicable a todos los niveles de Uriach, incluidos los órganos de dirección, los cargos directivos, los órganos de control y todo el personal.
c) El **ámbito relacional.** El ámbito de aplicación del presente Protocolo se extenderá, en la medida de lo posible, a proveedores, clientes, subcontratistas y empleados.
d) El **ámbito geográfico.** El presente Protocolo se aplicará a las actividades de Uriach en cualquier zona geográfica, ya sea local o internacional.

3. LEGISLACIÓN APLICABLE Y MARCOS DE REFERENCIA

Esta política se adapta a la siguiente normativa aplicable:

- Reglamento general de protección de datos (RGPD) 2016/679 de la UE, de 27 de abril de 2016, en lo sucesivo denominado "RGPD".
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; y demás normativa aplicable en materia de protección de datos en España, en adelante denominada "LOPDGDD".
- Normativa de protección de datos vigente en los países en los que Uriach o sus filiales desarrollan sus actividades.
- Normativa relativa a la protección de infraestructuras críticas.
- Marco Nacional de Seguridad (ENS) en las relaciones con el sector público.
- Código penal.
- Esta política utiliza los siguientes marcos de referencia:
- ISO/IEC 27001 Sistemas de gestión de seguridad de la información.
- ISO/IEC 27002 Código de buenas prácticas para los controles de seguridad de la información.

4. EN RELACIÓN CON EL COMPLIANCE

Esta política se ha elaborado conforme al Modelo de Compliance de Uriach, de acuerdo con la siguiente tabla de equivalencias.

Estructura reglamentaria	Las políticas, normas y procedimientos de seguridad de la información más relevantes se enumeran en el **ANEXO I** de esta política.
Estructura de control	La estructura de control de la seguridad de la información y la protección de datos se describe en la sección 6.
Organigrama	En el **ANEXO II** se indica la posición de los órganos de control de la protección de datos en el organigrama de Uriach.
Canal ético	Las infracciones de esta política y de las demás normas y procedimientos de este ámbito pueden denunciarse a través del canal Compliance de Uriach disponible en la intranet y en la página web de Uriach.
Sistema disciplinario	El incumplimiento se sancionará de acuerdo con el sistema disciplinario de Uriach.

5. OBJETIVOS Y PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Los objetivos de Uriach en materia de seguridad de la información están alineados con los de la empresa, y dan prioridad al cumplimiento de las obligaciones legales aplicables a la actividad que desarrolla.

Uriach tiene como objetivo prioritario en materia de seguridad de la información el cumplimiento del Reglamento general de protección de datos de la Unión Europea y de la normativa relativa a la protección de datos de carácter personal, así como cualquier otro tipo de reglamentación técnica en materia de datos confidenciales vigente en los países en los que opera. Por ello, todos los niveles de la organización están comprometidos con el cumplimiento de los objetivos marcados en materia de seguridad de la información y la aplicación de los controles corporativos establecidos.

La estrategia de seguridad de Uriach promueve el cumplimiento de los siguientes principios fundamentales:

- **Principio de confidencialidad**: la información solo debe ser accesible a los usuarios autorizados y no puede divulgarse a terceros sin autorización.
- **Principio de integridad**: los datos deben conservarse sin modificaciones no autorizadas y la información existente no debe ser alterada por personas o procesos no autorizados.
- **Principio de disponibilidad**: la información deberá ser accesible y poderse utilizar de forma permanente, garantizando la continuidad de los procesos y de las actividades.
    - Este principio va acompañado del principio de resiliencia: garantizar la resiliencia de los sistemas y la información tras un incidente que impida temporalmente el acceso.
- **Principio de autenticidad**: el origen y las identidades asociadas a la información son realmente los que aparecen en los atributos de la información.

- Este principio va acompañado del principio de no repudio: garantizar que un usuario no pueda negar la autoría de un acto en el sistema o la vinculación a un dato o conjunto de datos.

- **Principio de trazabilidad**: posibilidad de determinar siempre la identidad de las personas que acceden a la información y la actividad que realizan en relación con ella, así como los distintos estados y rutas que ha seguido la información.
- **Principio de proporcionalidad** entre los controles que deben aplicarse y la gravedad del riesgo que debe prevenirse, detectarse o mitigarse.

En los nuevos servicios y desarrollos se aplicará el principio de seguridad desde el diseño y por defecto.

6. ÓRGANOS DE CONTROL, FUNCIONES Y RESPONSABILIDADES

Uriach ha diferenciado las distintas funciones y responsabilidades en relación con el cumplimiento de la normativa aplicable en materia de protección de datos personales y seguridad de la información. Asimismo, todas las personas pertenecientes a Uriach, sea cual sea su cargo, están obligadas a cumplir las normas, procedimientos y controles establecidos en materia de seguridad de la información.

La estructura de control de Uriach está orientada a la prevención de riesgos relacionados con la seguridad de la información y, especialmente, a la prevención de infracciones que puedan suponer una vulneración de los derechos fundamentales de las personas en esta materia. Así, la estructura de control se basa en el siguiente esquema:

Consejo de Administración	El Consejo de Administración representa el nivel más alto de la estructura de control. Puede delegar funciones de control en los comités, departamentos y/o áreas de negocio y cargos que considere oportunos, con la única excepción de aquellas facultades que no puedan ser delegadas por ley.
Comité de Protección de Datos	El Comité de Protección de Datos es un órgano colegiado que, por delegación, asume las funciones atribuidas al DPD, según el RGPD. Se encarga de ejecutar, aprobar y actualizar el Registro de tratamiento, así como de elaborar y analizar los informes de auditoría. El Comité de Protección de Datos tiene una función preventiva del modelo de prevención descrito en esta política y tiene poderes autónomos de iniciativa y control.
Comité de Riesgos y Compliance	El Comité de Riesgos y Compliance define el modelo de cumplimiento de toda la organización y, entre otras cuestiones, trabaja en la gestión de riesgos para garantizar la continuidad de la empresa. El Comité de Riesgos y Compliance interactúa con el Consejo de Administración a través de la Comisión Delegada de Auditoria y Compliance.

DPD	El Delegado de Protección de Datos (DPD) asume la función de representar al Comité de Protección de Datos ante las autoridades, además de coordinar, acompañar y apoyar a los responsables de control de cada departamento y/o área de negocio, sobre los que recaerá la función de control.
Titular de los datos	El titular de los datos tiene el control administrativo y ha sido designado oficialmente como responsable de un conjunto de datos de activos de información específicos.
Responsable de seguridad	El responsable de seguridad se encarga de coordinar todos los esfuerzos de Uriach en materia de seguridad de la información.
Auditoría interna	El Departamento de Auditoría Interna tiene asignadas las funciones de control establecidas en esta política y en su propio reglamento.
Ejecutivos responsables de las funciones de control	Tanto los directores como los responsables de control tendrán asignadas sus funciones de control a través de los protocolos, normas y procedimientos que les afecten y, en la medida de lo posible, en la descripción de su puesto de trabajo.
Empleados con funciones de control	En algunos casos, las funciones de control pueden asignarse a empleados no directivos. La asignación de estas funciones se realizará a través de los protocolos, normas y procedimientos que les afecten y, en la medida de lo posible, en la descripción de su puesto de trabajo.

Uriach adoptará las medidas necesarias para que el personal conozca, de forma comprensible, las obligaciones en materia de protección de datos que afecten al ejercicio de sus funciones, así como las consecuencias de su incumplimiento.

7. OBLIGACIONES CONTRACTUALES

Además de los requisitos legales en materia de seguridad, Uriach está obligada a cumplir los requisitos específicos de seguridad exigidos por sus clientes y proveedores en relación con la información a la que puedan tener acceso en virtud de sus relaciones contractuales con los mismos.

En este sentido, Uriach identifica y actualiza aquellas obligaciones contractuales que puedan estar relacionadas con la seguridad de la información confidencial y los datos de carácter personal que trata o a los que accede. Asimismo, Uriach revisa y comprueba periódicamente que las obligaciones contractuales asumidas en materia de seguridad de la información sean conocidas en los niveles adecuados dentro de la organización, y que su alcance esté previsto en esta política y en las normas y procedimientos que la desarrollan.

8. RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Las actividades de Uriach incluyen la fabricación, venta, distribución y comercialización de productos sanitarios y farmacéuticos. Por lo tanto, los principales activos de Uriach son de naturaleza intangible y consisten en información confidencial, conocimientos especializados, datos personales, propiedad intelectual y propiedad industrial, entre otros.

La naturaleza intangible de estos activos los hace muy vulnerables a amenazas internas y externas, como, por ejemplo: i) el acceso no autorizado, ii) la copia no autorizada, iii) la divulgación, iv) la transferencia a terceros, v) el uso no autorizado, vi) la explotación no autorizada y vii) incluso la destrucción.

Asimismo, los riesgos relacionados con la seguridad de la información pueden adquirir criticidad penal, como delito tecnológico. Por ello, Uriach establece medidas de control dirigidas a mitigar, detectar y reaccionar ante la comisión de delitos relacionados con la privacidad personal y familiar, daños informáticos o la posible revelación de secretos de empresa.

Por ello, la protección de los activos de información requiere la adopción de una serie de medidas legales, técnicas y organizativas que se resumen en esta política y se detallan en las diferentes normas y procedimientos de Uriach.

En línea con lo anterior, Uriach realiza de forma periódica y continua un análisis de los riesgos y amenazas que afectan a la seguridad de la información.

El análisis de riesgos: i) parte de la definición de un mapa de riesgos inherentes, a través del cual se evalúa el riesgo existente antes de la aplicación de los controles de prevención, detección y reacción, y ii) genera un mapa de riesgos residuales, en el que se evalúan de forma automatizada los riesgos netos existentes tras la aplicación de los controles.

Por último, todos los niveles de la organización tienen la obligación de informar inmediatamente de cualquier riesgo detectado de incumplimiento de la normativa sobre protección de datos personales y seguridad de la información. Estos riesgos se comunicarán a través de los canales que Uriach tiene establecidos para comunicar todo tipo de riesgos de incumplimiento, preferentemente: canal Compliance de Uriach: Canal de denuncias anónimas - URIACH (report2box.com) o dpo@uriach.com para cualquier asunto relacionado con la violación de datos personales.

9. GESTIÓN DE ACTIVOS

Uriach realiza de forma periódica y continua un inventario de los activos materiales e inmateriales para determinar:

- su valor económico;
- su nivel de vulnerabilidad;
- su importancia para la empresa;
- la necesidad de aplicar medidas de seguridad para garantizar su protección.

Los activos deben tener asignado un código de identificación, que puede ser el número de serie en el caso de los activos físicos y un nombre único en el caso de los activos intangibles; asimismo, deben identificarse los servidores, las aplicaciones que contienen datos personales, los procesos y los ordenadores portátiles. En este sentido, Uriach dispone de un documento para la entrega y devolución de dispositivos corporativos. Además, todos los activos de los sistemas de información de Uriach están identificados en SAP.

10. CLASIFICACIÓN DE LA INFORMACIÓN

Uriach promueve la siguiente clasificación de la información para conocer el nivel de confidencialidad que debe aplicarse a cada documento y a cada tipo de datos:

- **Información confidencial:** información no pública de la organización o datos personales cuya divulgación podría causar perjuicios a Uriach o a terceros. Solo podrán acceder a la información confidencial, consultarla y utilizarla las personas expresamente autorizadas y dentro de los límites de la autorización. El círculo de personas autorizadas podrá incluir temporalmente a proveedores o clientes cuando exista una justificación clara o una obligación legal para ello.
- **Información para uso interno:** datos que no deben reproducirse ni comunicarse fuera del perímetro de Uriach. Solo el personal de Uriach podrá acceder a esta información, verla y utilizarla de acuerdo con los permisos que tenga en función de su puesto de trabajo.
- **Información pública:** sin restricciones de acceso, visualización o uso.

Así pues, por defecto, se considera confidencial toda la información que se encuentre dentro del perímetro de Uriach y, especialmente, la que se guarde en salas o armarios cerrados o en sistemas o aplicaciones protegidos con contraseña. Un documento o cualquier dato que se encuentre dentro del perímetro de Uriach no necesita estar marcado o sellado como confidencial para ser considerado confidencial.

En la medida de lo posible, los documentos y datos confidenciales llevarán un texto, etiqueta, sello o atributo que especifique el nivel de confidencialidad o seguridad que les corresponde. Los documentos o datos que no tengan esta característica también se considerarán confidenciales, a menos que pueda probarse su carácter público.

En caso de duda, el documento o dato no clasificado se considerará confidencial y se solicitará la autorización o aclaración pertinente respecto a su nivel de clasificación.

11. SEGURIDAD FÍSICA Y MEDIOAMBIENTAL

Uriach evalúa los riesgos y amenazas de su entorno. Esto incluye todas las fuentes de riesgo que puedan suponer un peligro para la seguridad de la información. Entre otras, son fuentes de riesgo:

- Infraestructuras críticas.
- Fábricas y empresas con actividades peligrosas.
- Depósitos de materiales inflamables.
- Depósitos de materiales explosivos.
- Líneas de alta tensión.
- Fuentes de radiofrecuencia.
- Garitas, cámaras y vallas.

Si Uriach gestiona o está próxima a una infraestructura crítica, tendrá en cuenta las medidas aplicables en la normativa de prevención de riesgos asociadas a este tipo de infraestructuras.

Asimismo, si resulta necesario y proporcional, se prevé la contratación de un servicio de alerta temprana que incluya avisos en relación con fallos en la red eléctrica o en las redes de comunicaciones, cambios en el nivel de alerta antiterrorista, fenómenos atmosféricos, catástrofes naturales y otras amenazas que puedan poner en riesgo la seguridad de las personas e infraestructuras de Uriach.

12. CONTROL DEL ACCESO FÍSICO

Uriach controla el acceso físico de las personas que acceden a sus instalaciones, que constituye el primer nivel del perímetro de protección de la seguridad de la información.

Este control puede realizarse directamente, a través de medidas técnicas y organizativas propias sobre las instalaciones en las que Uriach desarrolla su actividad, o a través de una empresa de vigilancia especializada en el control de accesos físicos.

Por otro lado, se entiende por segundo nivel de control de acceso físico el de las áreas, salas u oficinas en las que existen sistemas informáticos que albergan información confidencial o datos de carácter personal.

13. CONTROL DEL ACCESO DIGITAL

Uriach controla el acceso digital de las personas que acceden a los sistemas informáticos de la empresa. El control del acceso digital de las personas a los sistemas informáticos de la empresa se clasifica en distintos niveles de protección:

- **Primer nivel**: se centra en controlar el acceso a servidores, comunicaciones y cualquier otro canal que pueda utilizarse para la entrada y salida de información.
- **Segundo nivel**: ordenadores de sobremesa y terminales situados en Uriach.
- **Tercer nivel**: corresponde a los dispositivos móviles: ordenadores portátiles, teléfonos inteligentes y tabletas, entre otros.
- **Cuarto nivel**: basado en el control del acceso digital a las aplicaciones.

En línea con lo anterior, Uriach establece y verifica que los usuarios solo tengan acceso autorizado a los datos y recursos cuando lo necesiten con el fin de desempeñar sus funciones para la organización. Cada servidor y cada aplicación con información confidencial o datos personales gestiona la lista de usuarios y los perfiles y permisos de cada uno de ellos.

Asimismo, los sistemas operativos y las aplicaciones que se utilizan en el tratamiento deben disponer de mecanismos que impidan que un usuario acceda a recursos con derechos distintos a los autorizados.

Por último, los accesos y los accesos fallidos se registrarán en el registro correspondiente.

14. IDENTIFICACIÓN Y AUTENTICACIÓN

Uriach adopta medidas encaminadas a garantizar la correcta identificación y autenticación de los usuarios. Para ello, se establece un sistema que permite la identificación inequívoca de cualquier usuario que intente acceder a los recursos TIC de Uriach (PC, teléfonos móviles, tabletas, etc.) y comprobar que está autorizado.

En la medida de lo posible, las operaciones realizadas en la red corporativa o en la intranet de Uriach quedan registradas en los archivos de registro de los servidores. La utilización del identificador y la contraseña asignados a cada usuario implicará la aceptación, como prueba de la operación realizada, de los registros generados en dichos archivos de registro y almacenados en el sistema informático de Uriach. Salvo prueba en contrario, se presumirá que los actos realizados con el identificador y contraseña asignados han sido llevados a cabo por el usuario titular de los mismos.

15. GESTIÓN DE USUARIOS

Uriach tiene en cuenta los tipos de usuarios de la empresa, sus superiores y el gestor funcional de los recursos de los sistemas de información.

El tipo de usuarios depende de si se trata de un usuario interno o externo. Estos usuarios tienen un usuario superior y sus responsabilidades dependen del tipo de usuario del que son responsables.

Por último, existe un usuario responsable de los accesos con la función de autorizar el proceso de provisión de acceso a los recursos, asegurar el proceso de cancelación de acceso a los recursos, asegurar la actualización de los niveles de acceso a los recursos y revisar periódicamente los recursos que tiene bajo su responsabilidad.

16. CONTRASEÑAS

Uriach considera que la asignación, distribución y almacenamiento de contraseñas garantiza su confidencialidad e integridad.

Las contraseñas asignadas a cada usuario de la red corporativa son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse del uso indebido, divulgación o pérdida de las mismas. También deben seguir los siguientes criterios:

- La longitud mínima de la contraseña será de 8 caracteres.
- La contraseña deberá tener como mínimo una letra mayúscula, una letra minúscula, un número y caracteres especiales.
- La contraseña tendrá una fecha de caducidad de 90 días.
- No se podrá reutilizar ninguna de las 32 últimas contraseñas utilizadas.

El usuario no podrá comunicar ni compartir el identificador de usuario y la contraseña con ninguna otra persona. Salvo prueba en contrario, se presumirá que la actividad realizada con dicho identificador de usuario y contraseña ha sido llevada a cabo por el empleado titular de los mismos, quien asume toda responsabilidad laboral, civil o penal que pudiera derivarse de su uso.

17. SEGURIDAD LABORAL

La seguridad en el puesto de trabajo está regulada en las Normas de uso de los recursos TIC de Uriach. Cada ordenador dispone de un salvapantallas protegido por contraseña, que se activará tras un máximo de 5 minutos de inactividad.

Los usuarios aplicarán una política de escritorio limpio basada en la digitalización de su actividad y la eliminación del papel. Así, al final de la jornada laboral, los documentos que deban utilizarse en formato papel se guardarán en un armario cerrado con llave.

18. SEGURIDAD DE LAS APLICACIONES

Uriach mantiene y actualiza una lista de aplicaciones aprobadas, y no se puede instalar ni utilizar ninguna otra aplicación que no figure en esta lista. El proceso de aprobación de una solicitud tiene en cuenta:

- La seguridad de la aplicación y los riesgos que puede generar para la empresa, sus usuarios y terceros.
- El conocimiento y la fiabilidad de la fuente o el proveedor de la aplicación, de forma que no se pueda aprobar, instalar ni utilizar una aplicación que proceda de fuentes desconocidas o no identificadas o que no ofrezca garantías de calidad, seguridad y fiabilidad.

Uriach llevará un registro de las aplicaciones utilizadas en cada departamento. En este registro se describirán las medidas de seguridad establecidas en cada solicitud, que se verificarán con la lista de comprobación correspondiente y con la información facilitada por el proveedor. Asimismo, al iniciar el

desarrollo de una nueva aplicación, o la selección de una ya existente en el mercado, se evaluarán y considerarán las características que ofrece en materia de seguridad de la información.

Los usuarios no tendrán derechos de administrador sobre los ordenadores corporativos que utilicen, por lo que no podrán instalar aplicaciones sin autorización de Uriach.

Uriach tiene previsto implantar las herramientas tecnológicas necesarias para configurar filtros de URL, servidores proxy y otros sistemas y utilidades de red que impidan la descarga e instalación de aplicaciones no autorizadas.

Habrá un entorno de prueba para instalar y probar las principales aplicaciones empresariales antes de pasarlas a producción. Las pruebas previas a la implantación o modificación de una aplicación que trate datos personales no se realizarán con datos reales, sino con datos ficticios, a menos que se garantice el nivel de seguridad correspondiente al tratamiento. Si se prevén pruebas con datos reales, deberá haberse realizado previamente una copia de seguridad.

19. CONFIGURACIÓN SEGURA DEL SISTEMA

Uriach dispone y mantiene actualizado un protocolo que define las configuraciones adecuadas para que los sistemas de seguridad de Uriach sean seguros.

20. GESTIÓN DE EXCEPCIONES

Uriach establece normas de seguridad, pero están sujetas a cambios o posibles excepciones que deban aplicarse a los sistemas o activos propiedad de la organización. Uriach estudia y gestiona estas excepciones y dispone de un inventario de las excepciones comunes ya aprobadas.

21. GESTIÓN DE CAMBIOS Y CAPACIDADES

Uriach dispone de un protocolo que establece las directrices generales para garantizar un control adecuado de los cambios en los sistemas y servicios, y una correcta integración de la seguridad en los procesos de adquisición de sistemas y servicios. El objetivo es reducir el riesgo de fallos y garantizar la disponibilidad, además de establecer las directrices generales que deben tenerse en cuenta en la planificación de la capacidad y el rendimiento de los sistemas.

22. GESTIÓN DE PARCHES

Uriach dispone de un protocolo que proporciona directrices para la reparación de vulnerabilidades, de modo que los sistemas puedan protegerse adecuadamente y se garantice su seguridad y funcionamiento.

23. ARCHIVOS TEMPORALES

A efectos de esta política, son archivos temporales los archivos de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante el procesamiento.

Los archivos temporales y las copias de documentos que se hayan creado exclusivamente para la realización de trabajos temporales o auxiliares deben cumplir el nivel de seguridad que les sea aplicable. Todo archivo temporal o copia de trabajo así creados deben ser borrados o destruidos cuando ya no sean necesarios para los fines para los que fueron creados:

- Los archivos temporales creados automáticamente por las aplicaciones también serán eliminados automáticamente por las propias aplicaciones al final de la sesión.

- Los ficheros temporales generados por los sistemas operativos se eliminarán periódicamente gracias a los procesos automáticos de los propios sistemas operativos, dependiendo de su configuración, o manualmente, cuando sea necesario.

24. USO DE SOFTWARE CON LICENCIA

Uriach solo utiliza programas informáticos para cuyo uso se haya concedido una licencia. El uso de software sin licencia se considera una amenaza para la seguridad, así como una infracción de la propiedad intelectual.

Una vez al año, se realizará un inventario de software para determinar los sistemas operativos, utilidades y aplicaciones instalados en cada servidor, ordenador de sobremesa, portátil y dispositivo móvil de Uriach.

El inventario se cotejará con la lista de licencias contratadas por Uriach. Así, si el número de licencias es insuficiente, se analizará la conveniencia de desinstalar el software no cubierto por las licencias o adquirir las licencias que falten.

25. VIRUS Y MALWARE

Uriach establece medidas de seguridad para evitar la entrada de virus, malware y otras amenazas similares en los sistemas corporativos. Para ello, se instalan programas antivirus, antimalware y similares y se contratan los correspondientes servicios de actualización.

Asimismo, los usuarios reciben formación y advertencias adecuadas para saber cómo identificar, prevenir y evitar la entrada de virus y programas maliciosos a través de mensajes engañosos y técnicas de ingeniería social.

26. SEGURIDAD DE LAS COMUNICACIONES

Uriach lleva un registro de las redes de comunicaciones utilizadas, como Internet. Este registro describe las medidas de seguridad establecidas en cada red, que son objeto de controles periódicos.

Además, a la hora de seleccionar un nuevo proveedor de comunicaciones, se valorarán y tendrán en cuenta las características ofrecidas por el mismo en materia de seguridad de la información.

27. MEDIDAS DE CIBERSEGURIDAD Y SENSIBILIZACIÓN

Uriach establece medidas de ciberseguridad que incluyen la protección frente a amenazas de las redes de comunicaciones, como ciberataques, ataques de denegación de servicio, accesos no autorizados y secuestro de sistemas o *ransomware*, entre otros.

Asimismo, Uriach establece y mantiene actualizadas las medidas de seguridad adecuadas para evitar el correo no deseado (*spam*) y la recepción de mensajes que coincidan con el patrón de *phishing*. A este respecto, se prevé lo siguiente:

- **Impartir sesiones de formación y sensibilización** para el personal de mayor riesgo a fin de que aprendan a distinguir el *phishing* y las estafas que utilizan las redes de comunicaciones para realizar acciones no autorizadas, como transferencias de dinero y secuestro de ordenadores.
- **Envío de mensajes recordatorios** sobre los escenarios más comunes de engaño o ingeniería social. Por ejemplo:
    - Hacerse pasar por un directivo para pedir una información urgente y confidencial.
    - Suplantación de un proveedor solicitando un cambio de la cuenta corriente a la que deben transferirse los pagos de las facturas.

- Suplantación de un proveedor para enviar facturas falsas con una cuenta corriente diferente para pagarlas.

28. SEGURIDAD DE LA WIFI Y REDES INALÁMBRICAS

La red wifi de Uriach, así como cualquier otra red inalámbrica corporativa, cuenta con las medidas de seguridad necesarias para evitar accesos y usos no autorizados.

Uriach establece mecanismos para evitar que los usuarios de portátiles y dispositivos móviles corporativos, como smartphones y tabletas, accedan a redes wifi o a cualquier otro tipo de red inalámbrica que no sea conocida y fiable.

Los portátiles y dispositivos móviles corporativos también cuentan con medidas de seguridad reforzadas, como cortafuegos y VPN, para impedir el acceso no autorizado al dispositivo o a la información a través de las redes de comunicaciones que los usuarios utilizan cuando están fuera de Uriach. Además, para acceder a la red interna a través de la VPN, debe realizarse una autenticación multifactor (MFA).

29. DISPOSITIVOS MÓVILES

Uriach establece medidas de seguridad adecuadas para los dispositivos móviles corporativos y los dispositivos móviles personales autorizados para tener instaladas aplicaciones corporativas (BYOD).

Los usuarios a los que se asignen dispositivos móviles corporativos deben cumplir unas normas de uso específicas y aplicar las medidas de seguridad correspondientes.

Los usuarios de dispositivos BYOD también deben cumplir unas normas de uso específicas y aplicar las medidas de seguridad correspondientes para garantizar la seguridad de la información corporativa que se almacena en el propio dispositivo o a la que se accede a través de él.

30. TRABAJO FUERA DEL DOMICILIO Y RÉGIMEN DE TELETRABAJO

Uriach procura extender y reforzar los controles establecidos en materia de seguridad de la información para los recursos TIC corporativos o personales utilizados por los usuarios en sus domicilios particulares.

La práctica del teletrabajo debe ser aprobada por Uriach y garantizar el cumplimiento de la normativa laboral y de seguridad de la información. El jefe de cada departamento debe aprobar el teletrabajo para sus empleados.

Con las condiciones adicionales al contrato de trabajo se fijan los criterios sobre la responsabilidad de los usuarios y el tratamiento que debe darse a la información confidencial y a los datos personales.

En cualquier caso, debe garantizarse el nivel de seguridad correspondiente al tipo de datos tratados.

31. CONTROL DE PROVEEDORES CRÍTICOS

Uriach mantiene una lista actualizada de todos aquellos proveedores que tienen acceso directo o indirecto a datos personales o información confidencial. Incluye a todos los proveedores que pueden comprometer directa o indirectamente la seguridad de la información y que, por tanto, son considerados por la organización como proveedores críticos.

Se presta especial atención a la computación en la nube y a los proveedores de servicios de externalización, sobre todo cuando el tipo de funciones externalizadas es crítico para la empresa, o el proveedor asume una posición estratégica vital para la organización y para la continuidad de la

empresa. Asimismo, cuando sea necesario contratar un nuevo servicio que requiera acceso a datos, Uriach realizará una selección de proveedores y un proceso de evaluación y homologación que contemplará las medidas de seguridad necesarias para el tipo de datos que se van a tratar, que posteriormente se detallarán en el contrato. El proceso de selección y homologación de proveedores se basará en el proceso que Uriach ha desarrollado en materia de conformidad, añadiendo la evaluación de las medidas relativas a la seguridad de la información.

En esta evaluación, se dará prioridad a los proveedores que tengan la certificación ISO 27001 o se adhieran a otras normas en este ámbito. Esta certificación debe referirse específicamente al tipo de servicios que se van a contratar y a los servidores que alojarán los datos.

La relación con los proveedores que tengan acceso directo o indirecto a información confidencial y datos personales se regulará siempre en un contrato que incluirá: i) un apartado específico sobre medidas de seguridad de la información, ii) una regulación de los tiempos de respuesta del proveedor en un ANS específico para todo lo relacionado con la seguridad de la información.

Los proveedores deberán informar a la empresa Uriach con la que mantengan relación sobre cualquier tipo de subcontratación. Los subcontratistas están sujetos a los mismos requisitos que el proveedor principal y deben aplicar las mismas medidas de seguridad.

32. GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes y documentos que contengan información confidencial o datos personales deben identificar el tipo de información que contienen. Asimismo, como iniciativa, Uriach hará todo lo posible para elaborar un inventario, al que podrá acceder únicamente el personal autorizado, de los documentos que contengan información o datos de carácter personal. Al trasladar los soportes, deberán tomarse medidas para evitar el robo, la pérdida o el acceso indebido a la información durante el transporte.

Siempre que vaya a desecharse cualquier documento o soporte que contenga información confidencial o datos de carácter personal, deberá procederse a su destrucción o eliminación, adoptando las medidas destinadas a impedir el acceso a la información contenida en el mismo o su posterior recuperación.

La identificación de los soportes que contengan información confidencial o datos de carácter personal que Uriach considere especialmente sensibles podrá realizarse mediante sistemas de etiquetado comprensibles y significativos que permitan a los usuarios autorizados identificar su contenido y dificulten su identificación por parte de otras personas.

Deberá existir un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el remitente, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, que deberá estar debidamente autorizada.

Asimismo, deberá existir un sistema de registro de salida de soportes que permita conocer, directa o indirectamente, el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega, que deberá estar debidamente autorizada.

La distribución de soportes que contengan información confidencial o datos de carácter personal se realizará cifrando dichos datos o utilizando otro mecanismo que garantice que la información no sea accesible o manipulada durante su transporte o envío. Asimismo, se cifrarán los datos contenidos en dispositivos portátiles cuando se encuentren fuera de las instalaciones bajo control de Uriach.

Deberá evitarse el tratamiento de datos personales en dispositivos portátiles que no permitan cifrarlos. Si es estrictamente necesario, se justificará y se adoptarán medidas en función de los riesgos. En cualquier caso, Uriach podrá limitar el uso de soportes que contengan información confidencial y datos de carácter personal exclusivamente a aquellos que hayan sido aprobados, registrados y autorizados por la empresa.

33. COPIAS DE SEGURIDAD

Uriach realiza periódicamente copias de seguridad de la información para evitar su pérdida en caso de destrucción accidental o intencionada, y garantizar su reconstrucción en el estado en el que se encontraba en el momento de la pérdida o destrucción.

La frecuencia, el alcance, el lugar de conservación y el proceso de restauración de las copias de seguridad se describen en un procedimiento específico, y se puede contratar y auditar a un proveedor especializado en servicios de copias de seguridad.

34. CONTROL DE CANALES DE INFORMACIÓN DE ENTRADA Y DE SALIDA

Uriach establece controles para impedir la entrada y salida no autorizadas de información propia y de terceros. Para ello, se identifican los canales de entrada y salida de información, tanto digitales como analógicos, y se valora la adopción de controles si procede.

En esta línea, Uriach regula el proceso de selección y contratación de personal para evitar la entrada de información confidencial y datos personales de empleos anteriores. Asimismo, Uriach elabora y aplica un protocolo que regula el proceso de baja voluntaria y despido para evitar la salida de información confidencial, tanto propia como de terceros, y de datos de carácter personal.

35. ANONIMIZACIÓN, SEUDONIMIZACIÓN Y CIFRADO DE LA INFORMACIÓN

En la medida de lo posible, y cuando sea necesario, Uriach utilizará técnicas de disociación irreversibles o reversibles, basadas en la anonimización o seudonimización de los datos, así como el cifrado de los mismos, para proteger los derechos de las personas a las que se asocian y garantizar la confidencialidad.

- La **anonimización** consiste en la eliminación irreversible de los campos que permiten identificar a la persona física a la que se refieren los datos, mediante procedimientos adicionales que evitan o minimizan los riesgos de unicidad, vinculabilidad e inferencia.
- La **seudonimización** consiste en la supresión reversible de los campos que permiten identificar a la persona física a la que se refieren los datos, y su sustitución por un identificador que solo pueda asociarse al interesado con una tabla de equivalencias de acceso restringido.
- El **cifrado** se basa en un sistema de clave simétrica o asimétrica, siempre que la clave sea sólida y tenga la longitud y complejidad adecuadas, según el tipo de datos que se quiera ocultar.

36. CONTINUIDAD DE LA EMPRESA

Uriach prevé la aplicación de medidas para garantizar la continuidad de la actividad y la disponibilidad de la información corporativa y los recursos TIC. Estas medidas pueden incluir, entre otras:

- Un plan de emergencia con las medidas que deben adoptarse si un incidente de cualquier naturaleza impide el acceso a la información.
- Equipos alternativos, centros de procesamiento duplicados o proveedores con servicios o equipos que puedan sustituir al equipo principal en caso de avería o incidencia.

- Un protocolo de acceso a los documentos de trabajo de las personas ausentes para garantizar la continuidad de la actividad en el caso de directivos y empleados que se ausenten de la empresa durante un periodo prolongado por viaje, enfermedad, permiso de lactancia u otras situaciones similares.

Asimismo, Uriach aplicará las medidas necesarias para que los recursos TIC corporativos se encuentren en todo momento en correcto estado de funcionamiento y mantenimiento:

- En el caso del software, todos los sistemas operativos, aplicaciones, firmware y utilidades deberán estar actualizados con las últimas versiones, actualizaciones y parches de seguridad.
- En el caso del hardware, Uriach contratará los servicios de mantenimiento necesarios y dispondrá de equipos alternativos, centros de procesamiento duplicados o proveedores con servicios o equipos que puedan sustituir a los principales en caso de avería o incidencia.

37. SUPERVISIÓN DE RECURSOS INFORMÁTICOS (TIC)

Uriach dispone de un sistema de seguimiento de la actividad desarrollada en relación con los recursos TIC corporativos y los activos de información. Este seguimiento es automático y tiene, entre otros, los siguientes objetivos:

- Registro de la actividad con fines técnicos.
- Garantizar la integridad de la información.
- Identificación y prevención de posibles ataques de fuentes externas.
- Cumplimiento de las obligaciones legales o contractuales de trazabilidad.
- Detección de averías en los equipos.
- Recopilación de estadísticas.
- Prevención de la responsabilidad penal de Uriach.
- Registro de la actividad con fines forenses y probatorios.
- Registro de los cambios en el sistema.
- Garantía de la integridad de la información.
- Desarrollo de patrones de uso.
- Emisión de alertas sobre cambios en los patrones de uso.
- Detección de incumplimientos.
- Control de la entrada y salida de información.
- Garantía de la continuidad de la actividad.

Por último, en los casos en los que las alertas emitidas por el sistema hagan referencia a posibles usos indebidos, incumplimientos o infracciones, se aplicarán los correspondientes protocolos de investigación o inspección.

38. DESTRUCCIÓN Y BLOQUEO DE DATOS

Uriach dispone de un protocolo para la destrucción de la información que no sea necesario conservar o que ha superado el plazo establecido para su conservación. Este protocolo se aplicará a la siguiente área de material:

- Activos materiales e inmateriales.
- Medios digitales y analógicos.
- Información confidencial, información para uso interno e información no confidencial.

Por último, Uriach también impedirá el acceso a la información por parte de toda persona no autorizada, así como el tratamiento de los datos personales bloqueados.

39. GESTIÓN DE VULNERABILIDADES

Uriach dispone de un protocolo que proporciona directrices para reducir riesgos del sistema mediante una gestión eficaz de las vulnerabilidades. Para ello, se pondrá en marcha un programa de gestión de vulnerabilidades que incluirá, entre otras cosas, la identificación previa a la explotación, la evaluación de riesgos y la corrección de los mismos, con el fin de minimizar el impacto de los incidentes cibernéticos.

40. INCIDENTES DE SEGURIDAD

Uriach cuenta con un procedimiento de gestión de incidentes de seguridad que garantiza una respuesta inmediata ante cualquier amenaza que pueda surgir para la seguridad de la información. Asimismo, en el Anexo III se establece un protocolo de comunicación y gestión de incidentes de seguridad, así como la plantilla de notificación de incidentes de seguridad que los usuarios deben cumplimentar y remitir a los departamentos correspondientes para la resolución de cualquier incidencia.

Toda persona que tenga conocimiento o sospecha de un incidente que afecte a la seguridad de la información deberá comunicarlo inmediatamente a través de los canales establecidos al efecto. No comunicar un incidente de seguridad se considera una falta laboral grave.

41. CONTROLES PERIÓDICOS

En el ANEXO IV se detallan los principales controles periódicos que Uriach debe realizar para verificar el cumplimiento de esta política.

42. AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN

Si se considera oportuno, Uriach se someterá a una auditoría de seguridad de la información destinada a evaluar los riesgos contemplados en esta política. Esta auditoría podrá ser interna, externa o mixta, e incluirá una verificación de la existencia, adecuación y eficacia de las medidas de seguridad.

Dicha auditoría se realizará con carácter extraordinario siempre que se produzcan modificaciones sustanciales en los recursos TIC corporativos que puedan incidir en el cumplimiento de las medidas de seguridad establecidas para verificar la existencia, adecuación y eficacia de las mismas.

El informe de auditoría deberá evaluar el cumplimiento de la normativa externa e interna por parte de Uriach, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. También deberá incluir los datos, hechos, observaciones y pruebas en los que se basan las conclusiones alcanzadas y las recomendaciones propuestas.

43. INVESTIGACIONES E INSPECCIONES INTERNAS

Uriach podrá llevar a cabo una investigación o inspección internas de cualquiera de los recursos TIC corporativos.

- Las **investigaciones** tienen un ámbito de actuación más amplio que las inspecciones y pueden implicar a varios departamentos y/o áreas de negocio, procesos o equipos. Pueden realizarse en cualquier momento, de forma preventiva o tras la comunicación de un riesgo.
- Las **inspecciones** tienen un ámbito de actuación más limitado y deben basarse en una sospecha razonable de la existencia de un delito o una infracción de la normativa interna o externa.

44. FORMACIÓN Y SENSIBILIZACIÓN

Uriach promoverá la formación y sensibilización constantes en todos los niveles de la organización en materia de protección de datos y seguridad de la información. Esta actividad de formación adoptará la forma de un plan de formación que podrá incluir tanto sesiones presenciales como cursos de e-Learning.

La sensibilización puede basarse en cualquier tipo de material y herramientas de comunicación y formación para concienciar de los riesgos de infracción en todos los niveles de la organización.

45. ACTUALIZACIÓN Y MEJORA DE ESTA POLÍTICA

Esta política está sujeta a revisión y actualización continuas a fin de reflejar los cambios y mejoras introducidos en el ámbito de la protección de datos.

Asimismo, Uriach, a través de su Comité de Protección de Datos, realiza un seguimiento constante de la aplicación de las medidas de prevención y control, y propondrá, si procede, las modificaciones oportunas en los siguientes supuestos:

- Cuando salgan a la luz infracciones relevantes de esta política.
- Cuando se produzcan cambios significativos en Uriach o en la actividad que desarrolla.
- Cuando se produzcan cambios en los sistemas de información de Uriach.

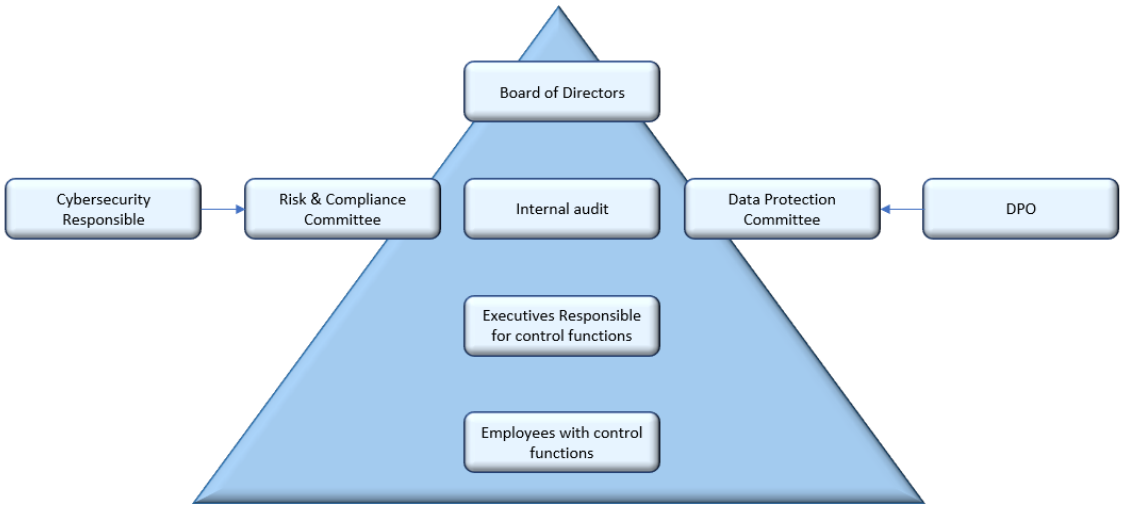
ANEXO I. LISTA DE LAS POLÍTICAS, NORMAS Y PROCEDIMIENTOS MÁS RELEVANTES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Política
Política de seguridad de la información

Protocolo
Gestión de activos
Clasificación de la información
Gestión de la prestación de servicios a proveedores
Requisitos de seguridad para contratos con terceros
Gestión de riesgos
Cumplimiento de los requisitos legales y contractuales
Gestión de vulnerabilidades
Requisitos de seguridad de los sistemas de información
Gestión de dispositivos extraíbles
Seguridad física
Seguridad de redes y comunicaciones
Copia de seguridad y recuperación
Gestión de accesos
Uso de controles criptográficos y firma electrónica
Identificación de usuarios y gestión de la autenticación
Auditorías de seguridad
Gestión de usuarios
Configuración segura del sistema
Gestión de excepciones
Gestión de cambios y capacidades
Gestión de parches
Transferencia de información
Sensibilización y formación
Seguridad de terminales
Seguridad en la nube
Continuidad de la empresa
Protección contra malware
Gestión y supervisión de registros
Gestión de incidentes de seguridad
Uso aceptable de los activos tecnológicos

Procedimientos
Gestión de activos
Gestión de vulnerabilidades
Copia de seguridad y recuperación
Gestión de accesos
Gestión de parches

ANEXO II. LOCALIZACIÓN DE LOS ÓRGANOS DE CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ORGANIGRAMA DE URIACH



ANEXO III. PROTOCOLO DE COMUNICACIÓN Y GESTIÓN DE INCIDENTES DE SEGURIDAD

Si se detecta un riesgo en cualquier nivel de Uriach, debe notificarse y gestionarse inmediatamente siguiendo el protocolo descrito a continuación.

Detección	Todos los niveles de la organización deben ser conscientes de que Uriach tiene un criterio de tolerancia cero en materia de riesgos relacionados con la seguridad, por lo que deben prestar atención a cualquier situación de riesgo que se detecte.
Comunicación	Una vez detectada una situación de riesgo, si está relacionada con datos, se comunicará inmediatamente al Comité de Protección de Datos a través de los canales establecidos al efecto: Si el riesgo está relacionado con el incumplimiento normativo, se comunicará al Comité de Riesgos y Compliance a través del canal Compliance de Uriach disponible en la intranet y en la página web de Uriach.
Registro	El Comité de Protección de Datos registrará la comunicación. En ningún caso se dejará desatendida una comunicación.
Evaluación	El Comité de Protección de Datos valorará la categoría del riesgo y determinará si se trata de un posible incumplimiento de la política de seguridad de la información o de una situación originada por causas ajenas a Uriach y a cualquiera de las personas que la integran.
Evaluación del riesgo para los derechos fundamentales de las personas	El Comité de Protección de Datos comprobará si ha habido riesgo para los derechos y libertades fundamentales de una persona o grupo de personas.
Archivo	Si el riesgo no es grave y no ha existido riesgo para los derechos y libertades fundamentales de una persona o grupo de personas, se procederá al archivo del expediente, sin perjuicio de las propuestas de mejora de las medidas de seguridad o de la política de seguridad que se estimen oportunas.
Notificación a la Agencia Española de Protección de Datos (AEPD)	Si se ha producido un riesgo para los derechos y libertades fundamentales, Uriach notificará a la AEPD el incidente de seguridad sin demora indebida y, a ser posible, en el plazo máximo de 72 horas desde que tuvo conocimiento del mismo. Si la notificación a la autoridad de control no se

	produce en un plazo de 72 horas, deberá ir acompañada de una indicación de los motivos del retraso. El contenido de la notificación será el establecido en el artículo 33 del RGPD.
Notificación a los interesados	Cuando sea probable que la violación de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, Uriach lo notificará al interesado sin dilaciones indebidas. La comunicación al interesado deberá describir, en un lenguaje claro y sencillo, la naturaleza de la violación de los datos personales, y contener al menos la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d). Antes de efectuar la comunicación, deberá comprobarse si se aplica alguna de las excepciones previstas en el artículo 34, apartado 3 del RGPD.
Cesión **Investigación** **Resolución**	Ante una posible violación o cualquier otra situación de riesgo relacionada con los datos de carácter personal, el Comité de Protección de Datos y el Comité de Riesgos y Compliance se encargarán de la investigación, adoptando las propuestas de mejora o sanciones que estimen oportunas, de acuerdo con lo establecido en la política de prevención y control.

PLANTILLA DE NOTIFICACIÓN DE INCIDENTES DE CIBERSEGURIDAD	
Sitio web, aplicación o servidor afectado	
Tipo de incidente	
Fecha de detección del incidente	
Fecha de inicio del incidente	
Fecha de finalización del incidente	
Datos personales afectados	
Medidas adoptadas	

ANEXO IV. CONTROLES PERIÓDICOS

Uriach planifica anualmente (plan de acción) los controles periódicos que debe realizar. Estos controles incluyen los que se enumeran a continuación:

1 Control de la aplicación de esta política

- Existencia de la política de seguridad en poder de los responsables de su aplicación.
- Nivel de conocimiento de las obligaciones de seguridad por parte de los usuarios.
- Nivel de cumplimiento de las obligaciones de seguridad por parte de los usuarios.
- Detección de incumplimientos.
- Necesidad de medidas correctoras.
- Necesidad de medidas disciplinarias.

2 Control del sistema de identificación y autenticación

- Nivel de actualización de la lista de usuarios autorizados.
- Nivel de actualización y adecuación de permisos concedidos.
- Funcionamiento correcto del sistema de identificación y autenticación.
- Cambio periódico de contraseñas.
- Almacenamiento cifrado de contraseñas.

3 Control del sistema de control de acceso

- Buen funcionamiento de los sistemas de control de acceso.
- Pruebas de intrusión.
- Comprobación del contenido de los registros.
- Configuración adecuada de los registros.
- Fiabilidad de los controles de acceso físico.
- Respeto de las limitaciones de acceso en función del puesto de trabajo o de la posición del usuario.
- Seguridad de las telecomunicaciones.

4 Control del cumplimiento de las normas de confidencialidad y secreto

- Clasificación de documentos.
- Respeto del nivel de confidencialidad de cada documento.
- Control de los canales de distribución de documentos.
- Nivel de sensibilización.
- Detección de incumplimientos.
- Necesidad de medidas correctoras.
- Necesidad de medidas disciplinarias.
- Verificación de las normas de cifrado en las telecomunicaciones.

5 Control de los procedimientos de gestión de soportes

- Identificación y etiquetado de soportes.
- Inventario de soportes.
- Almacenamiento seguro de soportes.
- Cumplimiento del procedimiento de autorización para la eliminación de soportes.
- Medidas que deben adoptarse cuando los soportes vayan a desecharse o reutilizarse.

- Funcionamiento de los registros de entrada y salida.
- Aplicación de medidas de seguridad a los soportes que abandonan la zona protegida.

6 Antivirus y control de malware

- Actualización periódica del software antivirus.
- Revisión de la automatización del control antivirus.
- Cumplimiento de las obligaciones de control antivirus.

7 Control del cumplimiento de las normas de propiedad intelectual

- Revisión de cada terminal mediante programas de auditoría de la red o del puesto de trabajo.
- Inventario de licencias de uso.
- Lista de software autorizado.
- Correlación entre las licencias existentes y los programas instalados.
- Control de contenidos y bases de datos.
- Necesidad de medidas correctoras.
- Necesidad de medidas disciplinarias.

8 Control del procedimiento de copia de seguridad

- Grado de cumplimiento de las obligaciones relativas a la realización de copias de seguridad.
- Grado de cumplimiento de la frecuencia establecida.
- Grado de cumplimiento de las obligaciones relativas al almacenamiento de copias.
- Grado de cumplimiento de las obligaciones relativas a las tareas de recuperación.

9 Control del procedimiento de gestión de incidentes de seguridad

- Grado de cumplimiento de la obligación de notificar los incidentes internamente.
- Grado de cumplimiento de la obligación de responder a los incidentes.
- Grado de cumplimiento de la obligación de registrar los incidentes.