Icalia Solutions

CÓDIGO DE BUENAS PRACTICAS EN SEGURIDAD

Declaración del Compromiso de Icalia Solutions SL

La dirección de Icalia Solutions SL, consciente de la importancia que la seguridad en el tratamiento de la información tiene para toda la organización, los accionistas, los clientes, los proveedores, y en general, todas las partes interesadas con las que se mantiene relación, ha considerado fundamental establecer el tipo de tratamiento que debe darse a la información de la que es propietaria o depositaria, durante todo su ciclo de vida y con el fin de garantizar su confidencialidad, integridad, y disponibilidad.

Uno de los objetivos prioritarios de Icalia Solutions SL y su dirección, es disponer de un sistema para la gestión de la seguridad de la información y de gestión de servicios, y como consecuencia de ello, obtener el más alto nivel de garantía en su tratamiento de la información y la correcta gestión de los servicios TI y que ello redunde en una mejora continua en nuestra relación interna y externa, logrando con ello que nuestros clientes perciban el compromiso de Icalia Solutions SL con respecto a la seguridad y a la calidad de los servicios ofrecidos.

ÍNDICE

1. Introducción

Este Código de Buenas Prácticas en Seguridad explica las normas de comportamiento que Icalia Solutions S.L. espera de usted en sus actividades profesionales en el manejo de la informacióny los sistemas de información.

Debe familiarizarse con las políticas corporativas que plasman directrices más detalladas sobre asuntos específicos que pueden afectar a su trabajo, tales como el código ético, calidad, respeto al medio ambiente, salud en el trabajo y recursos humanos.

Los sistemas de información suponen una infraestructura esencial para el desarrollo de la actividad de Icalia Solutions SL, y su Dirección así lo considera.

La naturaleza de la información gestionada por Icalia Solutions SL tiene un alto nivel de sensibilidad que requiere un cuidado especial en su tratamiento.

Como reconocimiento a este papel fundamental que los sistemas de información juegan en el desarrollo de los procesos de Grupo ICA y al especial cuidado requerido en el manejo de la información, este documento define las prácticas y normas de conducta habituales necesarias para la gestión y el uso seguro y responsable de la infraestructura de los sistemas de información de Icalia Solutions SL, haciendo especial hincapié en el uso de información de nuestros clientes y los datos de carácter personal.

Cambios en el contexto empresarial, en entorno legislativo o normativo, pueden crear la necesidad de modificar el Código, es por ello que la versión vigente del Código aparecerá en la versión electrónica en la Intranet de Icalia Solutions SL.

Audiencia

Este Código se dirige a todo el personal que desarrolle una prestación de servicio en Icalia Solutions SL[1] , que independientemente de su estatus, debe cumplir con la normativa para la seguridad de la información.

Ocasionalmente se podrían editar versiones personalizadas o reducidas, previamente autorizadas por el responsable de seguridad, dirigidas a perfiles de usuarios concretos como puedan ser usuarios especializados, administradores, clientes, proveedores, asesores externos, etc.

[1] En ICALIA el término empleados incluye a todos los trabajadores, incluyendo la Dirección de la empresa. Las funciones específicas de los empleados con funciones ejecutivas y control son desarrolladas en apartados concretos del Código.

Esta normativa se aplica a toda la información soportada por ordenadores, otros medios electrónicos y sistemas en red, administrados por Icalia Solutions SL, de los que ésta es propietario o depositario.

Del mismo modo, se aplicará a toda la información, independientemente de su formato o soporte (electrónico o papel).

La seguridad de la información no informatizada (fundamentalmente papel) y de aquélla contenida en soportes informáticos no corporativos (CD, DVD, discos duros de ordenadores personales, dispositivos USB, etc.) será responsabilidad de cada Área que deberá aplicar las medidas de seguridad apropiadas para garantizar lo establecido.

Aquellos trabajadores que desarrollan la actividad profesional en las instalaciones de clientes, colaboradores y otros terceros, deben aplicar aquellas prácticas de seguridad descritas en este documento, que no afecten negativamente o entren en contradicción con las políticas aplicadas en el entorno de trabajo.

2. Perfiles y responsabilidades

Las responsabilidades claves asociadas al presente Código son su entendimiento y su cumplimiento. El Código clarifica y explica las expectativas de Icalia Solutions SL respecto a sus empleados.

de Icalia Solutions SL ha desarrollado una estructura de responsabilidad a través de los Comités de Cumplimiento en diferentes niveles, que pasan por la asignación de responsabilidades acerca de la Seguridad, la Información, los Servicios y los Sistemas.

En base a este Código de Buenas Prácticas y con el fin de coordinar los esfuerzos, Icalia Solutions SL establece fundamentalmente dos roles, de los cuales, al menos uno será de aplicación a cada persona involucrada.

Estos roles son los siguientes: PROPIETARIOS y USUARIOS

Tales roles definen las responsabilidades generales con respecto a la protección de la información.

Propietarios

Los Propietarios de la información serán los responsables de los datos, incluidos los de carácter personal. Este papel lo desempeñan los Directores de Área y de Unidades de Negocio, a quienes se les asigna la responsabilidad de adquirir, desarrollar y mantener la información involucrada. A este grupo pertenecen

igualmente los Responsables de Tratamiento para la protección de datos de Carácter Personal, el Responsable de Seguridad, de los Servicios y los Sistemas.

Según el tipo de información, los Propietarios o personas delegadas clasificarán su nivel de confidencialidad (descrito más adelante), designarán los us uarios a los que se les permita el acceso y aprobarán las diversas formas en que la información será utilizada.

Usuarios

A esta categoría pertenece el resto de las personas involucradas. Corresponde a los Usuarios el responsabilizarse, familiarizarse y cumplir con toda la normativa de de Icalia Solutions SL, procedimientos, y estándares relacionados con la seguridad de la información. A este grupo pertenecen igualmente los Administradores de Sistemas y los usuarios de Datos de Carácter Personal.

Las cuestiones relacionadas con cómo gestionar de manera apropiada un tipo específico de información serán dirigidas a su Propietario.

Manejo consistente de la información

La información de de Icalia Solutions SL, o aquélla que le haya sido confiada, debe protegerse según su nivel de confidencialidad. Deben emplearse medidas de seguridad independientemente del soporte en que la información esté almacenada (papel, soportes magnéticos u ópticos, etc.), sistema en que se procese (ordenadores personales, dispositivos portátiles, smartphones, buzones de voz, etc.), o medio por el que se transporte (correo electrónico, correo convencional, mensajería, conversación cara a cara, etc.).

La información debe protegerse de forma eficaz, independientemente del punto en el que se encuentre en su ciclo vital, desde su origen hasta su destrucción.

Responsabilidad de las copias de seguridad

El *Departamento de Sistemas* realiza copias de la información corporativa contenida en todos los sistemas centrales, así como de las unidades de red habilitadas para los usuarios.

Los Usuarios tienen la responsabilidad de salvaguardar la información no informatizada o aquélla que conteniéndose en soporte informático no ha sido considerada ni corporativa ni de especial sensibilidad y que reside únicamente en soportes fuera del control del *Departamento de Sistemas* (principalmente, discos duros de los ordenadores de los puestos personales).

Toda copia de seguridad de Usuarios es almacenada con la codificación o controles de acceso físico correspondientes, en un lugar apropiado y nunca

podrá ser extraída, por ningún medio ni bajo ningún concepto, sin la autorización expresa y documentada del Propietario de la información.

Deber de secreto

Los Usuarios tienen la obligación de mantener indefinidamente, incluso una vez finalizada la relación con Icalia Solutions SL, la absoluta reserva y sigilo sobre cualquier información a que accedan en el ejercicio de sus funciones, según se establece en las políticas desarrolladas, el contrato que vincula las partes, en la legislación aplicable y el convenio colectivo.

3. Clasificación de la información

La información de de Icalia Solutions SL, o aquélla que le haya sido confiada, debe protegerse según su sensibilidad.

Toda la información bajo control de Icalia Solutions SL, tanto si ha sido generada interna o externamente se distinguirá dentro de estas categorías.

Icalia Solutions SL no aplica por defecto un modelo de etiquetado, pero el esquema de Clasificación de la información es lógico y la información es fácilmente identificable por su naturaleza:

- CONFIDENCIAL
  Se aplica a documentación que debe ser conocida sólo por algunos usuarios concretos, y cuya divulgación no autorizada podría impactar seria y adversamente a Icalia Solutions SL, sus clientes, sus socios comerciales, y/o sus proveedores. Además pertenecen a este nivel los considerados como categoría especiales de datos según la legislación de protección de datos, aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.
  Ejemplos de este tipo de documentación son los contratos laborales de los empleados, balances financieros, planes estratégicos, contratos especiales, información de proyectos, código fuente, ofertas de clientes, las credenciales de acceso a sistemas e instalaciones, etc.
- SOLO PARA USO INTERNO
  Se aplica a documentación que debe ser conocida sólo por el personal de la compañía, o por el personal de algunos departamentos concretos, y aunque su divulgación no autorizada va en contra de este procedimiento, no impacta seria o adversamente a de Icalia Solutions SL, *sus clientes, sus socios comerciales, y/o sus proveedores. A esta categoría pertenecen los datos*

de carácter personal, que por su naturaleza no han sido incluidos en la categoría Confidencial. Ejemplos de este tipo de documentación son contactos, políticas y procedimientos, contratos genéricos, agenda de contactos, etc.

- PÚBLICA
  Se aplica a la documentación que puede ser conocida por el público en general. Por definición, no existe la difusión no autorizada para este tipo de documentación y por lo tanto puede ser difundida sin que produzca un daño potencial. Ejemplos de este tipo de documentación son las presentaciones comerciales de servicios y productos, la información corporativa de la Web de Icalia Solutions SL, etc.

Todo el personal deberá familiarizarse con las definiciones de estas categorías y niveles y con los procedimientos a seguir para la seguridad de la información según la categoría y el nivel al que pertenezca.

En este Código de Buenas Prácticas, "información sensible" es aquella que pertenece a la categoría confidencial o a categoría especiales de datos personales, según lo establecido en el Reglamento General de Protección de Datos.

4. Manejo de la información

La información de Icalia Solutions SL, o aquélla que le haya sido confiada, debe tratarse de acuerdo a principios proporcionales de seguridad.

No toda la información requiere del mismo nivel de protección, para ello se desarrollan unas guías generales sobre cómo utilizar la información en función de su clasificación.

Información sensible

Acción	***Requisito***
Almacenamiento soporte fijo	Control de acceso lógico y físico.
Almacenamiento soporte removible	Cifrado o mecanismo que impida su acceso.
Almacenamiento en papel	Bajo llave.
Copia	Se requiere la autorización del Propietario.
Fax	Verificar los datos y la disponibilidad del destinatario.
Envío por red pública	Cifrado o mecanismo que impida su acceso.
Destrucción	Destructora de documentos, de soportes o contenedores seguros.
Envío a terceras partes	La autorización previa del Propietario o existencia de acuerdo de confidencialidad firmado.
Etiquetado de copias en papel	Paginación y fecha.

Etiquetado de embalajes para envío	Dirección especifica del destinatario en el embalaje, pero sin la etiqueta de clasificación visible.
Concesión de derechos de acceso	Autorización previa del Propietario.
Registros y trazabilidad	De envío.

Información de uso interno

Acción	***Requisito***
Almacenamiento en soporte fijo	Control de acceso lógico.
Almacenamiento soporte removible	Mecanismo que impida su acceso.
Almacenamiento en papel	En armarios o cajoneras cerrados.
Copia	Se requiere haberlo notificado documentalmente al Propietario.
Fax	Verificar los datos y la disponibilidad del destinatario.
Envío por red pública	Verificar la lista de distribución.
Destrucción	Contenedores de reciclado.
Envío a terceras partes	La autorización previa del Propietario o existencia de acuerdo de confidencialidad firmado.
Etiquetado de copias en papel	Versión y fecha.
Etiquetado de embalajes para envío	Dirección especifica del destinatario en el embalaje, pero sin la etiqueta de clasificación visible.
Concesión de derechos de acceso	Autorización previa del Propietario.
Registros y trazabilidad	No se requiere.

Información de uso público

Acción	***Requisito***
Almacenamiento en soporte fijo	Sin restricciones.
Almacenamiento soporte removible	Sin restricciones.
Almacenamiento en papel	Sin restricciones.
Copia	Sin restricciones.
Fax	Sin restricciones.
Envío por red pública	Sin restricciones.
Destrucción	Contenedor de reciclado.
Envío a terceras partes	Sin restricciones.
Etiquetado de copias en papel	Sin restricciones.
Etiquetado de embalajes para envío	Sin restricciones.
Concesión de derechos de acceso	Sin restricciones.
Registros y trazabilidad	No se requiere.

Aquellos usuarios que requieran de alguno de los tratamientos relacionados en los apartados anteriores y no disponga de los medios adecuados, deberá contactar con el superior jerárquico para su solicitud o recibir las instrucciones adecuadas de tratamiento.

5. Accesos

El acceso a la información que es propiedad o está bajo el control de Icalia Solutions SL está restringido por mecanismos y prácticas que se limitan a las personas que están autorizadas.

Acceso basado en la necesidad de saber

El acceso a la información que es propiedad o está bajo el control de Icalia Solutions SL se permitirá según la necesidad de conocimiento. En otras palabras, sólo se les permitirá acceso a aquellos que tengan una necesidad legítima de tal información para el desarrollo de su trabajo.

Del mismo modo, los trabajadores no deben impedir o retener el acceso a la información cuando el Propietario de la información en cuestión dé instrucciones de compartirla.

No está permitido a los trabajadores intentar acceder a la información sensible sin la previa aprobación de derechos de acceso por parte del Propietario.

Cuando un trabajador varía sus tareas (incluyendo traslado, la finalización de contrato, ascenso o excedencia), su correspondiente responsable directo deberá notificarlo inmediatamente al Director de Área afectada, así como al *Departamento de Sistemas* para la revocación o modificación de sus derechos de acceso.

Icalia Solutions SL podrá conceder accesos temporales a la información autorizada por el/los Propietario/s. Estas situaciones se corresponden habitualmente con aquéllas en las que una actividad se puede ver interrumpida por bajas laborales temporales, finalización contractual, disfrute de vacaciones, con el objeto de darcontinuidad a las actividades.

Identificadores de usuario y contraseñas

Icalia Solutions SL, para facilitar la aplicación de las medidas de seguridad y la facilidad en el desarrollo del trabajo de los usuarios de sus sistemas, ha implantado sistemas de identificación y autenticación única, a través de la identificación de los usuarios en el acceso a los ordenadores de trabajo, no obstante para aquellos sistemas o aplicaciones que por cualquier causa requieran de intervención adicional de usuario con identificador o contraseña, deberán seguir los principios de buena práctica reflejados en este documento.

Para implementar el proceso de Necesidad de Conocimiento, cada trabajador con acceso a los sistemas informáticos tendrá un único nombre de usuario y contraseña privada, personal e intransferible.

Estos nombres de usuario servirán para restringir privilegios basándose en las tareas del puesto, responsabilidades de proyecto y otras actividades administrativas. Cada usuario es personalmente responsable del uso de su nombre de usuario y contraseña y de todas las actividades que con ellos se realicen.

PERSONAL - SECRETA - INTRANSFERIBLE
FÁCIL DE RECORDAR - DIFÍCIL DE AVERIGUAR

Recomendaciones

Aunque en los sistemas que lo permiten, se han incluido políticas restrictivas que obligan a buenas prácticas en la selección y vigencia de contraseñas, para asegurar que los sistemas de protección de acceso cumplen el papel que les corresponde, los usuarios deberán elegir contraseñas que sean difíciles de adivinar. Esto es, la contraseña no debe estar relacionada con la vida personal o profesional ni estar basada en palabras de diccionario.

Un guía útil para la selección de las contraseñas puede estar basado en las siguientes características:

1. Longitud mínima: 7 caracteres
2. Combinación de distintos tipos de caracteres:
   a. Letras mayúsculas
   b. Letras minúsculas
   c. Dígitos
   d. Caracteres especiales o no alfanuméricos Ej: +=-_%(ááí.
3. NO se permiten:
   a. contraseñas que incluyan el identificador del usuario
   b. secuencias fácilmente identificables, por ejemplo: 1234, aaaa, asdf.
   c. palabras que estén en un diccionario, nombres de personas y fechas
4. Será fácil de recordar, pero difícil de averiguar:
   a. Una palabra sin sentido, o un anagrama de una frase.
   b. Una clave que no pueda olvidar, para evitar escribirla en alguna parte.
5. Ejemplos de contraseñas robustas y fáciles de recordar:
   a. 2Huevos+Jamón
   b. SiempreALa2ª
   c. 40º=GripeA
   d. H2O=agua
   e. Sin1€aDía20

Almacenamiento

Las contraseñas no deben almacenarse en ningún medio legible, no deben escribirse de forma alguna que puedan ser identificadas fácilmente, ni dejarse en algún lugar donde personas sin autorización puedan descubrirlas.

En caso de que el trabajador necesite anotar la contraseña en un papel, deberá custodiar este papel con las mismas precauciones y el mismo celo con el que custodiaría su tarjeta de crédito bancaria o su DNI.

6. En relación con el personal

La dirección cuenta con la colaboración de todos sus empleados y asume la responsabilidad de motivar, concienciar, y formar adecuadamente a todos ellos. Éstos están en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en este código.

Protección contra robos

Los ordenadores y dispositivos portátiles deberán asegurarse cuando se extraigan de las oficinas, no perdiendo su control o situándolos bajo llave en armarios o cajoneras, o utilizando cualquier otro sistema de cierre que los proteja, teniendo el usuario la obligación de notificar lo antes posible ante cualquier incidente o pérdida.

No está permitido extraer equipos informáticos de Icalia Solutions SL fuera de sus límites físicos, sin que la persona en cuestión haya recibido la correspondiente autorización o esta utilización forme parte de sus obligaciones laborales. Las agendas personales, los teléfonos móviles y otros dispositivos que están, por s u función, definidos como dispositivos portátiles, no están incluidos en este apartado.

Ten en cuenta que los dispositivos que salen de la organización y almacenan información sensible deben estar debidamente protegidos. Si no estás seguro de la protección aplicada, consulta a tu superior o con el *Departamento de Sistemas*.

Puestos de trabajo

Los puestos de trabajo están bajo la responsabilidad de los usuarios, que garantizarán que la información que utilizan no pueda ser visible por personas no autorizadas. Esto implica que tanto la documentación en papel, como pantallas, impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar situados físicamente de manera que garanticen esa confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de la información sensible, apagando su ordenador, forzando el protector de pantalla o el bloqueo de la sesión. Igualmente, no se dejarán sobre la mesa soportes con información sensible. Ningún dispositivo (impresoras, pantallas, etc.) debe permanecer funcionando al finalizar el turno de trabajo a menos que sea necesario para el normal funcionamiento de Icalia Solutions SL.

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos sensibles. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo imprimidos.

Se recomienda la revisión periódica de los archivos y borrar aquéllos que no tengan ninguna utilidad, observando minuciosamente lo que al efecto marquen las normas legales.

Los usuarios son los primeros responsables de toda información que esté compartida para otros usuarios en sus carpetas compartidas, siendo de éstos la obligación de verificar la compartición de estos archivos periódicamente.

Registro de actividad de los Sistemas

Los sistemas de información para el desempeño de las funciones de los usuarios son propiedad de Icalia Solutions SL y deben ser, por tanto, destinados a tal fin.

Con el fin de asegurar el cumplimiento de la normativa interna y las leyes y regulaciones aplicables, Icalia Solutions SL registra en ficheros de log e inspecciona la actividad que se desarrolla en sus sistemas. Los usuarios deben conocer que la utilización de herramientas de registro de actividad y contenidos es habitual en los sistemas de información.

Denuncia obligatoria

Todas las supuestas violaciones de la normativa, intrusiones al sistema, infecciones de virus y otras condiciones que supongan un riesgo para la información o los sistemas informáticos de Icalia Solutions SL, deberán ser inmediatamente notificadas al superior jerárquico.

En caso de pérdida o revelación de información sensible a personas no autorizadas o sospecha fundada de estas acciones, se deberá notificar inmediatamente al Propietario de la información o al Responsable de Seguridad.

Las incidencias relacionadas con la seguridad deben dirigirse al centro de soporte de Icalia Solutions SL < dpd@icalia.es > o a través de las herramientas que Icalia Solutions SL ponga a disposición de los usuarios.

7. Uso de sistemas

La empresa, previa autorización documentada del responsable del trabajador, pondrá a disposición de los empleados cuyo trabajo así lo requiera, los pertinentes equipos informáticos y otros sistemas de información, tales como ordenadores,

impresoras, teléfonos fijos, smartphones y otros medios necesarios para el desarrollo de la actividad profesional.

Cuando accedes a los Sistemas de Información propiedad de Grupo ICA que permiten hacer uso del Sistema Informático, las Redes, la Información y los Servicios, debes conocer que al hacerlo aceptas las políticas y buenas prácticas de uso de estos activos, las políticas de Calidad, Medio Ambiente, Seguridad de la Información y Servicios Gestionados, y te comprometes a cumplir y a hacer cumplir todos los principios de seguridad que la dirección ha establecido, garantizando la protección de la información en todo momento, y evitando y colaborando a que la continuidad del negocio sea mantenida de forma permanente.

De acuerdo al interés legítimo, garantizar la obligación legal del cumplimiento de los compromisos contractuales con clientes, socios y/o proveedores, con la finalidad de conocer el estado de avance o ejecución de las tareas de los trabajadores en situaciones de imperiosa necesidad, como pueden ser en caso de enfermedad, situación de baja prolongada, excedencia o finalización de la relación laboral, la empresa podrá acceder a los equipos informáticos y a otros sistemas de información puestos a disposición de los empleados.

Configuración

Los puestos de trabajo tendrán una configuración en sus aplicaciones y sistemas operativos que sólo podrá ser alterada por el *Departamento de Sistemas.*

No está permitida la modificación de la configuración básica de sistemas operativos o programas suministrados con los equipos y que pueden provocar conflictos con la utilización de determinados servicios de la red.

Correo electrónico

Icalia Solutions SL facilita a cada usuario que lo necesite, una cuenta de correo electrónico para el mejor desarrollo de su actividad profesional.

Los usuarios deben revisar sistemáticamente las carpetas de mensajes y borrar todos los que no sean necesarios.

Los trabajadores han de ser conscientes de que el correo electrónico corporativo forma parte de la imagen de la compañía, y que algunos contenidos, manifestaciones y expresiones de la correspondencia electrónica de los empleados mediante el correo corporativo, pero con fines particulares pueden comprometer y afectar negativamente la imagen de la compañía.

En consecuencia, en el caso de que, durante su jornada laboral, y por razones de necesidad, los empleados tuvieran que hacer razonablemente uso del correo

electrónico para fines privados, los empleados deberán utilizar sus cuentas de correo electrónico particulares.

La herramienta de correo electrónico solo debe ser utilizada para las tareas relacionadas con el puesto de trabajo. No está permitida la emisión de correos en cadena o pirámide que puedan saturar los sistemas informáticos, dificultar los trabajos de mantenimiento, o puedan suponer un perjuicio en la imagen corporativa.

Cualquier fichero introducido en la red o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas, debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y propiedad de datos de carácter personal.

Debes ser consciente que los ficheros adjuntos protegidos por contraseñas o mecanismos similares no pueden ser verificados por el sistema antivirus por lo que una vez descomprimidos deben ser escaneados manualmente por el usuario antes de su utilización.

Acceso a Internet

El uso del sistema informático de Icalia Solutions SL para acceder a las redes públicas como Internet, se limita a los temas directamente relacionados con la actividad profesional y los cometidos del puesto de trabajo del usuario.

El acceso a páginas *web* con contenido ilícito, nocivo, pornográfico, etc., es especialmente peligroso ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido salvo autorización expresa.

El acceso a las páginas *web*, grupos de noticias y otras fuentes de información se limita a aquellos que contengan información relacionada con la actividad profesional o con los cometidos del puesto de trabajo del usuario.

Debes ser consciente que los ficheros descargados a través de páginas consideradas seguras (cuya dirección empiezan por 'https') no pueden ser verificados directamente por el sistema antivirus perimetral por lo que una vez descargados deben ser escaneados manualmente por el usuario.

Uso razonable

En general, los equipos fijos o por portátiles, smartphones y sistemas de comunicación están destinados a ser utilizados con fines relacionados con el negocio. No obstante, el uso personal es admisible si el mismo no consume más de una cantidad trivial de recursos, no interfiere con la productividad de los trabajadores, no interfiere con cualquier actividad del negocio, no es utilizado

para la extracción no autorizada de información y no causa problemas jurídicos a la organización o a sus trabajadores.

Como consecuencia de todo lo anterior, los empleados no pueden albergar ninguna expectativa razonable de confidencialidad ni de intimidad en el uso de los equipos informáticos, dispositivos electrónicos y de comunicación, correo electrónico corporativo, acceso a internet, y otros medios propiedad de Icalia Solutions SL, ni siquiera en aquellos casos en los que, conforme a lo expuesto anteriormente, la compañía tolera el uso moderado y razonable de dichos equipos y dispositivos con fines particulares.

8. Actividades no permitidas

Las actividades deliberadas contra estos objetivos serán tratadas de acuerdo a la legislación y a la relación contractual existente en cada momento.

No son prácticas autorizadas

- Compartir o facilitar el identificador de usuario y la clave de acceso con cualquier persona o ceder la sesión activa de su usuario a un tercero sin presenciar la actividad que este realice.
- Intentar modificar los registros y configuración del sistema, incluida la instalación de sistemas operativos no homologados.
- Intentar descifrar claves, algoritmos de cifrado, contraseñas y cualquier otro elemento de seguridad de los sistemas de información.
- Extraer información interna sin la previa autorización del Propietario o del Responsable de Seguridad.
- Utilizar recursos no homologados, discos virtuales o almacenamiento en la nube de propiedad ajena a Icalia Solutions SL para tratar información del negocio.
- Destruir, alterar, inutilizar o dañar de cualquier otra forma los datos, programas o documentos informáticos propios o de terceros, sin la autorización explícita del Propietario.
- Obstaculizar voluntariamente el acceso de otros usuarios a la red, mediante el consumo masivo de recursos informáticos, así como realizar acciones que dañen, interrumpan o generen errores en los sistemas.
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos propios o de terceros.
- Intentar aumentar ilícitamente el nivel de privilegios de un usuario.
- Instalar voluntariamente programas ajenos, malware o cualquier otro dispositivo lógico que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos propios o de terceros.

- Desinstalar, desactivar o impedir la actualización de los programas antimalware que evitan la entrada en el sistema de cualquier elemento destinado a destruir, alterar o extraer datos.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos y cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la organización, en la red y sistemas corporativos.
- Representar a las marcas, a la imagen, o actuar u opinar en nombre de Icalia Solutions SL en medios públicos, foros, redes sociales de forma no autorizada.
- El tratamiento de datos personales fuera del ámbito de las funciones y responsabilidades asignadas, especialmente aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, genéticos, biométricos, relativos a la salud o a la vida sexual o la orientación sexual de una persona.

9. Gobierno del código

Icalia Solutions SL ha puesto en marcha una estructura de gobierno para garantizar que se promocionan los principios del Código a través de la empresa y que el mismose aplica de forma eficaz.

Estructura organizativa

La estructura organizativa de la gestión de la seguridad de la información está compuesta por los siguientes agentes:

- El Comité de Cumplimiento de Icalia Solutions SL
- El Responsable de Seguridad

Además de la colaboración del resto de actores que pueden intervenir en los procesos relacionados con la gestión de los Servicios.

Comité de Seguridad de Icalia Solutions SL

El Comité para la Gestión y Coordinación de la Seguridad de la Información está integrado en el Comité de Cumplimiento de Icalia Solutions SL, cuya composición puede consultarse en el Código Ético de Icalia Solutions SL.

Cómo informar acerca de una infracción

Cualquier persona que trabaje para Icalia Solutions SL, o cualquier cliente, proveedor, socio u otras terceras personas, que tenga conocimiento de una posible infracción del Código tiene la importante obligación de informar de ello.

Si quiere hacer una pregunta, necesita asesoramiento o tiene base para creer que se ha infringido una de las disposiciones del presente Código, o que puede que usted lo haya incumplido, deberá hablar lo antes posible con alguna las siguientes personas:

- ☐ *Recursos Humanos rrhhbcn@grupoica.com*
- ☐ *Responsable de Seguridad dpd@icalia.es*
- ☐ *Delegado de Protección de Datos dpd@icalia.es*
- ☐ *Responsable de Cumplimiento canaleticobcn@grupoica.com*

10. Penalizaciones por infracciones

No respetar intencionadamente el Código de Buenas Prácticas en Seguridad o la legislación aplicable puede conducir a adoptar medidas disciplinarias proporcionadas a la infracción, incluyendo la finalización del contrato de trabajo. Los empleados que incumplan la ley se exponen ellos mismos, y a la Sociedad, a las sanciones penales (tales como multas y prisión) o civiles (tales como daños y perjuicios o penalizaciones).

Departamento de recursos humanos
C/Almogàvers 119-123, Plt.2ª Ofi.1ª Distrito 22@ 08018
Barcelona
93 452 02 65
rrhh@icalia.es