Anexo XI

Protocolo de Seguridad de la Información

Aprobado por el Consejo de Administración de ACS Servicios, Comunicaciones y Energía, S.A. el 16 de diciembre de 2020

Índice

1. Definiciones

- **ACS**: ACS, ACTIVIDADES DE CONSTRUCCIÓN Y SERVICIOS, S.A., sociedad cabecera del Grupo ACS.
- **ACS SCE**: ACS SERVICIOS, COMUNICACIONES Y ENERGÍA, S.A., sociedad cabecera del Grupo ACS Industrial.
- **ACS Industrial o la organización:** Grupo ACS Industrial. Incluye a la matriz, ACS SCE, y a las distintas divisiones[1] de ésta, así como sus respectivas filiales y las UTE's en las que se encuentren sociedades del Grupo.
- **CNS**: Cuerpo Normativo de Seguridad, conjunto de documentos a diferentes niveles que conforman los requerimientos, directrices y protocolos que debe seguir el Grupo ACS.

2. Introducción

Las divisiones de ACS SCE y sus correspondientes filiales que conforman ACS Industrial se adhieren a la Política de Seguridad de la Información aprobada por el Consejo de Administración de ACS el 14 de agosto de 2020. Dicha Política persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de negocio de las sociedades que componen el Grupo ACS.

[1] COBRA GESTIÓN DE INFRAESTRUCTURAS, S.A.U. ("**COBRA**"); CONTROL Y MONTAJES INDUSTRIALES CYMI, S.A. ("**CYMI**"); CYMI BRASIL, S.L.U. ("**CYMI BRASIL**"); DRAGADOS OFFSHORE, S.A. ("**DRAGADOS OFFSHORE**"); ELECTRICIDAD ELEIA, S.L.U. ("**ELEIA**"); ENCLAVAMIENTOS Y SEÑALIZACIÓN FERROVIARIA, S.A.U. ("**ENYSE**"); ELECTRONIC TRAFFIC, S.A. ("**ETRA**"); IMESAPI, S.A. ("**IMESAPI**"); INITEC ENERGÍA, S.A. ("**INITEC**"); INTECSA INGENIERÍA INDUSTRIAL, S.A. ("**INTECSA**"); MAETEL INSTALACIONES Y SERVICIOS, S.A ("**MAETEL**"); MAKIBER, S.A. ("**MAKIBER**"); MANTENIMIENTO Y MONTAJES INDUSTRIALES, S.A. ("**MASA**"); SOCIEDAD ESPAÑOLA DE MONTAJES INDUSTRIALES, S.A. ("**SEMI**"); y SICE TECNOLOGÍAS Y SISTEMAS, S.A. ("**SICE**").

Esta Política de Seguridad de la Información es la pieza angular por la que se rige el CNS del Grupo ACS. El CNS deberá ser desarrollado por cada división de ACS Industrial mediante un conjunto de documentos (normas de uso, estándares normativos, procedimientos, manuales, guías, buenas prácticas, etcétera) de tal manera que cubran todos los aspectos, llegando a nivel de proceso operativo.

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

2.1 Objetivo

El objetivo principal del presente Protocolo es definir los principios y las reglas básicas para la gestión de la seguridad de la información. El fin último es lograr que las divisiones de ACS Industrial garanticen la seguridad de la información y minimicen los riesgos de naturaleza no financiera derivados de un impacto provocado por una gestión ineficaz de la misma.

2.2 Alcance

El Protocolo es aplicable para todas las divisiones de ACS Industrial, que deberán cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible. Adicionalmente, las divisiones de ACS Industrial deberán adaptar y desarrollar este Protocolo en sus filiales y deberán reportar a la matriz de ACS Industrial su adecuación a dicho Protocolo, en ejecución de los procesos de monitorización del sistema de gestión de Cumplimiento Normativo de ACS Industrial. El alcance del presente Protocolo abarca toda la información de las divisiones de ACS Industrial con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

El Protocolo deberá ser informado en la página web corporativa de cada división y estar disponible en un repositorio común de la división correspondiente, de forma que sea accesible por todas las personas.

2.3 Adaptación y desarrollo por parte de las divisiones del Protocolo

Este Protocolo de Seguridad de la Información ha sido adaptado para su aplicación a cada una de las divisiones de ACS Industrial. Cada división decidirá la manera en la que adapta el Protocolo a su operativa mediante documentación concreta, es decir, su CNS, que siempre deberá estar alineada con las directrices que se marcan en el presente documento.

En consecuencia, cada una de las divisiones de ACS Industrial deberá usar el Protocolo definido en el presente documento como requisito mínimo y adaptarla a sus condiciones y manera de trabajar, mediante diferentes tipos de documentación, para conseguir definir los requisitos de seguridad a nivel operativo.

3. Principios del Protocolo de Seguridad de la Información

El presente Protocolo responde a las recomendaciones de las mejores prácticas de seguridad de la información recogidas en el Estándar Internacional ISO/IEC 27.001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la seguridad de la información, puedan afectar a ACS Industrial.

Además, ACS Industrial establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- Alcance estratégico: La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de las divisiones de ACS Industrial de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- Seguridad integral: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

- Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.
- Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

ACS Industrial considera que las funciones de seguridad de la información deberán quedar integradas en todos los niveles jerárquicos de su personal.

Puesto que la seguridad de la información incumbe a todo el personal de ACS Industrial, este Protocolo deberá ser conocido, comprendido y asumido por todos sus empleados.

Para la consecución de los objetivos de este Protocolo, ACS Industrial deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, ACS Industrial mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

4. Compromiso de la Dirección

La Dirección de ACS Industrial, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación del Protocolo de Seguridad de la Información entre los empleados de ACS Industrial.
- Exigir el cumplimiento del Protocolo, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

5. Roles y responsabilidades

ACS Industrial se compromete a velar por la seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas normativas y leyes aplicables.

Cada división de ACS Industrial deberá nombrar una figura responsable de definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información. Esta figura deberá establecerse desde un entorno de gobierno y gestión, y tendrá entre sus funciones y responsabilidades el aplicar principios de segregación de funciones y el contacto con las autoridades y grupos de interés especiales en materia de seguridad de la información.

La figura asumirá las funciones que, con carácter general, sean atribuidas por el presente Protocolo de Seguridad de la Información a dicha figura.

Será su responsabilidad desarrollar y mantener el Protocolo, asegurándose que ésta sea adecuada y oportuna según evolucione tanto la división de ACS Industrial de la que sea responsable como la regulación vigente.

6. Gestión de la seguridad de los Recursos Humanos

El departamento de Recursos Humanos deberá realizar su gestión teniendo en cuenta los criterios de seguridad establecidos en el Protocolo de Seguridad de la Información, siendo éste un punto clave para asegurar su cumplimiento.

Se deberán salvaguardar los requisitos establecidos en el presente Protocolo en todo momento, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desistimiento de contratos de los empleados.

6.1 Formación y concienciación

ACS Industrial deberá asegurar que todo el personal recibe un nivel de formación y concienciación adecuado en materia de seguridad de la información en los plazos que exija la normativa vigente, especialmente en materia de confidencialidad y prevención de fugas de información.

Asimismo, los empleados deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de manera que pueda garantizarse el cumplimiento de este Protocolo.

Por otro lado, los empleados tienen la obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

6.2 Política de mesas limpias

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.
- Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Esto incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, guardando bajo llave los que por su clasificación sean confidenciales o secretos (véase el Anexo: Niveles de clasificación).

- Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

7. Gestión de activos

Se deberán tener identificados e inventariados los activos de información necesarios para la prestación de los procesos de negocio de ACS Industrial. Adicionalmente, se deberá mantener actualizado el inventario de activos.

Se deberá realizar la clasificación de los activos en función del tipo de información que se vaya a tratar, de acuerdo con lo dispuesto en el apartado *8. Clasificación de la información*.

Se deberá asignar un Responsable encargado de realizar la gestión propia de los activos de información durante todo el ciclo de vida. El Responsable deberá mantener un registro formal de los usuarios con acceso autorizado a dicho activo.

Además, para cada activo o elemento de información deberá existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido.

Se deberán actualizar de manera periódica las configuraciones de los activos para permitir el seguimiento de estos y facilitar una correcta actualización de la información.

7.1 Gestión de dispositivos BYOD o dispositivos personales

ACS Industrial permitirá la política conocida como BYOD (Bring Your Own Device), que permite a los empleados utilizar sus recursos o dispositivos móviles personales para acceder a recursos o información de la organización.

Adicionalmente, los usuarios deberán tener en cuenta una serie de requisitos establecidos en este Protocolo:

- Se deberán aplicar las mismas medidas y configuraciones de seguridad a los dispositivos BYOD que tratan información igual que al resto de dispositivos de ACS Industrial.
- El usuario será responsable de los equipos BYOD.

- Los usuarios deberán mantener actualizado el dispositivo BYOD personal donde traten información de cualquier tipo de ACS Industrial. Asimismo, deberán tener instaladas aplicaciones de seguridad (antivirus, antimalware, etcétera) para evitar brechas de seguridad en esos equipos.
- Los empleados deberán comunicar previamente a su Responsable de área la utilización de los dispositivos BYOD.

7.2 Gestión del ciclo de vida la información

ACS Industrial deberá gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases.

El ciclo de vida de un activo de información consta de las siguientes fases:

1. Creación o recolección: esta fase se ocupa de los registros en su punto de origen. Esto podría incluir su creación por un miembro de ACS Industrial o la recepción de información desde una fuente externa. Incluye correspondencia, formularios, informes, dibujos, entrada/salida del ordenador u otras fuentes.
2. Distribución: es el proceso de gestión de la información una vez que se ha creado o recibido. Esto incluye tanto la distribución interna como externa, ya que la información que sale de ACS Industrial se convierte en un registro de una transacción con terceros.
3. Uso o acceso: se lleva a cabo después de que la información se distribuya internamente, y puede generar decisiones de negocio, generar nueva información, o servir para otros fines. Detalla el conjunto de usuarios autorizados por ACS Industrial a acceder a la información.
4. Almacenamiento: es el proceso de organizar la información en una secuencia predeterminada y la creación de un sistema de gestión para garantizar su utilidad dentro de ACS Industrial. Si no se establece un método de almacenamiento para la presentación de información, su recuperación y uso resultaría casi imposible.

5. Destrucción: establece las prácticas para la eliminación de la información que ha cumplido los periodos de retención definidos y la información que ha dejado de ser útil para ACS Industrial. Los periodos de conservación de la información deberán estar basados en los requisitos normativos, legales y jurídicos que afectan a ACS Industrial. También deberán tenerse en cuenta las necesidades de negocio. Si ninguno de estos requisitos exige que la información sea conservada, deberá ser desechada mediante medios que garanticen su confidencialidad durante el proceso de destrucción.

ACS Industrial deberá identificar medidas de seguridad de acuerdo con el presente Protocolo para asegurar la correcta gestión del ciclo de vida de los activos.

7.3 Gestión de las copias de seguridad

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar periódicamente. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros y bases de datos con una periodicidad, al menos, semanal, salvo que en dicho período no se hubiese producido ninguna actualización. En su caso, se podrá establecer una frecuencia más alta de realización de copias de seguridad, si la información a salvaguardar es de impacto alto para ACS Industrial y/o de elevado nivel de transaccionalidad.

Como normal general, la frecuencia con la que se realizarán las copias de seguridad se determinará en función de la sensibilidad de las aplicaciones o datos, de acuerdo con los criterios de clasificación de información declarados en el anexo “Niveles de clasificación”.

Las copias de seguridad deberán recibir las mismas protecciones de seguridad que los datos originales, asegurándose su correcta conservación, así como los controles de acceso adecuados.

Como norma general y siempre que sea posible, se deberá requerir que la información en las copias de seguridad esté cifrada. Este requerimiento será obligatorio para determinados tipos de información confidencial.

Se deberán realizar pruebas de restauración de las copias de seguridad disponibles y de los procesos de restauración definidos, a fin de garantizar el funcionamiento correcto de los procesos. Estas se realizarán de forma periódica y quedarán documentadas.

Se deberá establecer un período de retención de las copias de seguridad hasta su destrucción una vez terminado el periodo de existencia.

Las copias de seguridad, tanto de archivos maestros como de aplicaciones y archivos de información se deberán ubicar en lugares seguros con acceso restringido. Asimismo, las copias de respaldo se ubicarán preferentemente en un centro distinto al que las generó.

8. Clasificación de la información

En cada división, el Responsable de área deberá definir un modelo de clasificación de la información que permita conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad. El modelo de clasificación deberá integrar los requisitos y condiciones establecidos en el presente apartado del Protocolo.

El Responsable de área de cada división será el encargado de su actualización cuando se crea conveniente, así como de dar a conocer el modelo de clasificación a todos los empleados de su ámbito de actuación.

8.1 Tipos de información

ACS Industrial deberá clasificar la información en función del soporte en el que está siendo utilizado:

a) Soportes lógicos: información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información desarrollados a medida o adquiridos a un tercero.

b) Soportes físicos: información que esté en papel, soportes magnéticos como USBs, DVDs, etcétera.

8.2 Niveles de clasificación

En función de la sensibilidad de la información, ACS Industrial deberá catalogar la información en cinco niveles, véase la definición precisa en el Anexo “Niveles de clasificación”:

- Uso público
- Difusión limitada
- Información confidencial
- Información reservada

- Información secreta

8.3 Gestión de información privilegiada

La información que se considere reservada, confidencial o secreta se deberá tratar con especial cuidado. Se deberán definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada. Este tipo de información se deberá enviar cifrada y mediante protocolos seguros.

8.4 Etiquetado de la información

ACS Industrial deberá etiquetar mediante métodos manuales o, en la medida de lo posible, automatizados para facilitar el procesamiento adecuado de las medidas de seguridad que apliquen en cada caso.

Se deberán etiquetar los documentos o materiales, así como los anexos, copias, traducciones o extractos de estos, según los niveles de clasificación de la información definidos en el subapartado anterior, exceptuando la información considerada de “Uso público”.

Se deberá definir un proceso o procedimiento para el etiquetado de la información de acuerdo con los siguientes requisitos:

- Asegurar que el etiquetado de la información refleja el esquema de clasificación de la información adoptado.
- Asegurar que las etiquetas sean fácilmente reconocibles entre todos los empleados.
- Orientar a los empleados sobre dónde y cómo se colocarán o utilizarán las etiquetas, en función del proceso de acceso a la información o a los activos que la soportan.
- Indicar las excepciones en los que se permite omitir el etiquetado, sin que ello suponga una omisión del deber de clasificar la información.

Se deberá prestar especial atención y tratar con cuidado máximo el etiquetado de activos físicos que contengan información reservada o secreta, para evitar su sustracción por ser fácilmente identificable.

Se deberán establecer las medidas técnicas, si fueran necesarias, y viables de etiquetado automático de la información soportada en medios digitales.

ACS Industrial deberá asegurar la formación y capacitación de todos sus empleados en el etiquetado de la información, así como formar y capacitar específicamente a los empleados que traten información de nivel reservada o secreta.

8.5 Manipulación de la información

ACS Industrial se encargará de desarrollar e implementar un conjunto adecuado de procedimientos para la correcta manipulación de la información. Se deberán adoptar las medidas necesarias para proteger la información de acuerdo a su clasificación.

La información confidencial o secreta estará en todo momento custodiada durante todo el ciclo de vida de la misma.

8.6 Privacidad de la información

ACS Industrial deberá asegurar la privacidad de los datos de carácter personal con el objetivo de proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la propia imagen, mediante el establecimiento de medidas para regular el tratamiento de los datos.

ACS Industrial deberá cumplir con la legislación vigente en materia de protección de datos personales en función de la jurisdicción en la que esté establecida y opere (a modo ilustrativo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantías de los Derechos Digitales para el caso de España) y deberá incluir las medidas necesarias para cumplir con la normativa.

Se deberán implementar medidas adecuadas para asegurar la privacidad de la información en todas las fases de su ciclo de vida (de acuerdo con el apartado *7.2. Gestión del ciclo de vida de la información)*.

9. Prevención de fugas de información

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

Se deberán analizar los vectores de fuga de información, en función de las condiciones y operativa de trabajo de cada división de ACS Industrial. Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo para cada sociedad, basándose en la criticidad del activo y el nivel de clasificación que la información tenga. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos en sus diferentes estados del ciclo de vida.

ACS Industrial deberá definir procedimientos para evitar la ocurrencia de las situaciones que puedan provocar la pérdida de información, así como procedimientos de actuación en caso de que se notifique una fuga de información.

Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- Proceso para el manejo de dispositivos de alta criticidad conocidos
- Uso adecuado de dispositivos extraíbles como USBs, CD/DVDs o similares
- Uso del correo electrónico
- Transmisión de información de forma oral
- Impresión de documentación
- Salida de documentación
- Uso de dispositivos móviles
- Uso de Internet
- Escritorios limpios y ordenados (véase el apartado 6.2. Política de mesas limpias)
- Equipos desatendidos

10. Control de acceso

Todos los sistemas de información de ACS Industrial deberán contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.

El control de acceso se entenderá desde la perspectiva tanto lógica (enfocado a sistemas de la información) como física (véase el apartado 12. Seguridad Física y del Entorno).

10.1 Requisitos de negocio para el control de acceso

ACS Industrial deberá asumir una serie de requisitos de negocio para el control de acceso, que serán, al menos, los siguientes:

- Los usuarios deberán ser únicos y no podrán ser compartidos. Asimismo, los privilegios de los usuarios serán inicialmente asignados mediante el principio de mínimo privilegio.
- Se prohibirá el uso de usuarios genéricos. En su defecto, se utilizarán cuentas de usuario asociadas a la identidad nominal de la persona asociada.

10.2 Derechos de acceso

ACS Industrial deberá implementar controles de acceso que garanticen que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.

Los derechos de acceso deberán ser establecidos en función de:

- Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.
- Necesidad de saber: Solo se permitirá el acceso a un recurso cuando exista una necesidad legítima para el desarrollo de la actividad.
- Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.
- Segregación de funciones: deberá asegurarse una correcta segregación de funciones para desarrollar y asignar derechos de acceso.

Asimismo, ningún usuario deberá poder acceder por sí mismo a un sistema de información controlado sin la aprobación del Responsable del propio usuario (o de la persona designada).

10.3 Control de acceso lógico

ACS Industrial deberá establecer una política de contraseñas adecuada y alineada con las buenas prácticas en seguridad. La política de contraseñas definirá los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña.

La política de contraseñas deberá ser conocida por todos los empleados de ACS Industrial.

10.4 Teletrabajo

Se deberá controlar el acceso remoto a la red de las divisiones de ACS Industrial en la modalidad de trabajo a distancia, esto es, desde fuera de las instalaciones propias.

Los servicios de conexión al trabajo en remoto estarán destinados exclusivamente a personal de ACS Industrial. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del Responsable de Seguridad.

El equipo utilizado para la conexión en la modalidad de trabajo en remoto podrá ser propiedad del empleado o proporcionado por ACS Industrial. En cualquier caso, es obligatorio que el equipo cumpla con los siguientes requerimientos de seguridad:

a) Capacidad de realizar una conexión a través de una VPN.

b) Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.

c) Software antivirus instalado.

d) Software de firewall/cortafuegos personal instalado.

El teletrabajo desde un equipo propio del trabajador requerirá de todas las medidas de seguridad oportunas, con el objetivo de que el trabajo en remoto no suponga una amenaza para la seguridad de la información de ACS Industrial. Además, se podrán establecer medidas de seguridad adicionales a las existentes para asegurar de una manera más fiable la conexión segura en remoto.

El servicio de teletrabajo se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad.

11. Gestión del ciclo de vida de la identidad

Las divisiones de ACS Industrial deberán definir e implementar un adecuado sistema de gestión del ciclo de vida de la identidad. La identidad es el conjunto de características que identifican de forma unívoca a toda persona con acceso físico o lógico a los sistemas de información de ACS Industrial. El ciclo de vida de la identidad es el proceso que sigue la identidad de un usuario desde su creación hasta su eliminación.

El ciclo de vida de la identidad se compone de las siguientes actividades:

a) Creación y asignación de la identidad

b) Revisión periódica

c) Modificación o eliminación

La gestión de este ciclo requiere definir los requisitos de seguridad y responsabilidades de cada una de las etapas, con el objetivo de centralizar y facilitar los procesos de gestión asociados a las mismas.

La gestión del ciclo de vida de la identidad deberá estar alineado con el Departamento de RR.HH. con el objetivo de verificar las identidades en función de las altas y las bajas de empleados y su correspondencia en los sistemas de información.

11.1 Identidades Privilegiadas

La asignación y uso de derechos de acceso privilegiado deberá estar restringida y controlada. El acceso privilegiado es el acceso a sistemas como administrador o con un rol que ofrezca la posibilidad de modificarla configuración del sistema.

La asignación de derechos de acceso privilegiado deberá ser controlada a través de un proceso formal de autorización de acuerdo con las políticas de control de acceso. Deberán considerarse, al menos, los siguientes requisitos:

- Deberán identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso (por ejemplo, sistema operativo, sistema de gestión de base de datos o aplicación), así como los usuarios a los que estos les deberán ser asignados.
- La asignación de derechos de acceso privilegiados deberá realizarse en base a las necesidades de uso, basándose en el mínimo privilegio y necesidad de saber.

- Deberá definirse un proceso de autorización que incluya un registro de los privilegios asignados. No deberán concederse derechos de acceso privilegiado hasta que el proceso de autorización se complete.
- Deberán definirse los requisitos para la caducidad de los derechos de acceso privilegiado.
- Las competencias de los usuarios con derechos de acceso privilegiado deberán revisarse regularmente con el objetivo de verificar que se encuentran alineadas con sus obligaciones.
- Deberán establecerse y mantenerse procedimientos y mecanismos específicos para evitar el uso no autorizado de cuentas de usuario genéricas para la administración, conformes con las capacidades de configuración de los sistemas.
- Se deberán establecer procedimientos y mecanismos que aseguren la confidencialidad de la información secreta de autenticación para los usuarios genéricos de administración (por ejemplo, modificación frecuente de contraseña, mecanismos de compartición de la contraseña seguros, etcétera).

12. Seguridad Física y del Entorno

Los espacios físicos donde se ubiquen los sistemas de información de ACS Industrial deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas de manera que puedan evitarse o mitigar el impacto de incidentes de Seguridad (accesos no autorizados a sistemas de información, robo o sabotaje) y accidentes ambientales (incendios, inundaciones, cortes de suministro eléctrico, etcétera).

Además, el Responsable de área de cada división deberá garantizar que existe un control de acceso a la información que se encuentre en formato físico mediante un registro sobre quién accede a la información. Por otra parte, la información confidencial se deberá almacenar con medidas específicas como armarios ignífugos.

13. Seguridad en trabajo en la nube o cloud

ACS Industrial deberá mantener una política de trabajo en la nube o cloud computing que establezca las medidas de seguridad adecuadas para la confidencialidad, integridad y disponibilidad de la información. Dependiendo de tipo de modelo de servicio en la nube, se deberán aplicar diferentes medidas de seguridad:

- Infraestructura: en primer lugar, se deberá asegurar que el Proveedor monitoriza el entorno para detectar cambios no autorizados. Además, se deberán establecer fuertes niveles de autenticación y control de acceso para los administradores y las operaciones que estos realicen. Por último, las instalaciones y/o configuraciones de los elementos comunes deberán estar registrados y conectados con el objetivo de obtener la trazabilidad adecuada.
- Plataforma: de forma adicional a las medidas indicadas en el modelo de servicio de Infraestructura, el Proveedor del servicio deberá proporcionar mecanismos de seguridad correspondientes al ciclo de vida del software seguro, de acuerdo con el apartado 15. Seguridad en el ciclo de vida del desarrollo de sistemas.
- Software: de forma adicional a las medidas indicadas en el modelo de servicio de Plataforma, ACS Industrial y el Proveedor deberán seguir OWASP (Open Web Application Security) como guía para la seguridad de las aplicaciones.

14. Seguridad en la operativa

Todos los sistemas de información de ACS Industrial que procesan o almacenan información de su propiedad deberán contar con las medidas de seguridad oportunas que optimicen su nivel de madurez adecuado (monitorización, control de cambios, revisiones, etcétera). Asimismo, se deberán gestionar, controlar y monitorizar las redes de manera adecuada, a fin de protegerse de las amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluidos los controles de acceso a la red, protegiendo así toda la información que se transfiera a través de estos elementos y/o entornos.

15. Seguridad en las telecomunicaciones

La arquitectura de red de ACS Industrial deberá contar con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. Se entiende por “dominio interno” la red local compuesta por los elementos tecnológicos de ACS Industrial accesibles exclusivamente desde la red interna. Por otra parte, se entiende por “dominio externo” la red accesible desde el exterior de la red de ACS Industrial.

Es de suma importancia la administración de seguridad de las redes que atraviesan el perímetro de ACS Industrial, implantando controles adicionales para los datos sensibles que circulen por las redes de comunicación públicas.

Por ello, ACS Industrial definirá las pautas de seguridad a seguir con relación a la transferencia de información, así como las medidas de seguridad en la utilización de equipos portátiles, servicios de Internet y correo electrónico, y de controles específicos que permitan una conexión segura a los sistemas de información de ACS Industrial desde fuera de sus instalaciones.

16. Seguridad en el ciclo de vida del desarrollo de sistemas

Toda la adquisición, desarrollo y mantenimiento de los sistemas deberá contar con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas del sector. Además, deberá realizarse una gestión de las pruebas, el seguimiento de los cambios, y el inventario del software.

Cada departamento de la división de ACS Industrial deberá tener en cuenta la seguridad de la información en sus procesos de sistemas y datos, procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

17. Seguridad en los Proveedores

Se deberá poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad de negocio.

Sobre los proveedores de estos servicios se deberán cuidar los procesos de selección, requerimientos contractuales como la terminación contractual, la monitorización de los niveles de servicio, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en el presente Protocolo.

18. Gestión de Incidentes

Todos los empleados de ACS Industrial tienen la obligación y responsabilidad de la identificación y notificación al Responsable de Seguridad de la división correspondiente de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, ACS Industrial deberá implementar procedimientos para la correcta gestión de los incidentes detectados.

Se deberá definir un procedimiento de gestión de respuesta ante incidentes, en el que se defina un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

19. Continuidad de Negocio

Respondiendo a requerimientos de calidad y buenas prácticas, ACS Industrial deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la sociedad actúe en caso de ser necesario. Este Plan de Continuidad deberá ser actualizado y probado periódicamente. Además, se deberá definir y mantener actualizado un Plan de Recuperación ante Desastres alineado con la continuidad de negocio, este plan abarcará la continuidad del funcionamiento de las tecnologías de información y comunicación.

ACS Industrial deberá encargarse de la formación y capacitación para todos sus empleados en materia de Continuidad del Negocio. La formación en materia de Continuidad del Negocio deberá ser revisada periódicamente con el objetivo de estar totalmente alineada con el Plan existente.

20. Cumplimiento regulatorio

ACS Industrial deberá comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

21. Gestión de Excepciones

Cualquier excepción al presente Protocolo de Seguridad de la Información deberá ser registrada e informada al Responsable de Seguridad de la Información de la división de ACS Industrial que corresponda. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la sociedad y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los Responsables del negocio.

22. Sanciones disciplinarias

Cualquier violación del presente Protocolo de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de cada división de ACS Industrial. Es responsabilidad de todos los empleados de ACS Industrial notificar al Responsable de Seguridad de la Información de la sociedad afectada cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por el presente Protocolo.

23. Revisión del Protocolo

La aprobación de este Protocolo implica que su implantación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, así como para cumplir también con todos sus requisitos.

El presente Protocolo de Seguridad de la Información, será revisado y aprobado por el Consejo de Administración cuando corresponda. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que el Protocolo permanece adaptado en todo momento a la realidad de ACS Industrial.

24. Anexos

24.1 Anexo: Niveles de clasificación

Nivel	Detalle Nivel	Ejemplos
Uso público	Se trata de la información que puede ser conocida por cualquier tipo de persona y su utilización fraudulenta no supone un riesgo para los intereses de ACS Industrial.	Son ejemplos de este tipo de información los catálogos de productos y la información disponible en la web corporativa de cada división.
Difusión limitada	Es la información utilizada por las áreas de ACS Industrial y cuya utilización fraudulenta supone un riesgo para los intereses de ACS Industrial poco significativo.	Son ejemplo de este tipo de información los correos electrónicos y los documentos de trabajo de las áreas de ACS Industrial.
Información Confidencial	Es aquella información que solo puede ser conocida por un número reducido de personas y para la que un uso fraudulento puede suponer un impacto para los intereses de ACS Industrial significativo.	Son ejemplos de este tipo de información los informes de auditoría y de estrategia de ACS Industrial.
Información Reservada	Es aquella información que únicamente debe conocer el propietario de la misma, así como, en casos concretos, un grupo muy reducido de personas. La revelación o divulgación no autorizada de este tipo de información puede causar graves perjuicios para los intereses de ACS Industrial.	Son ejemplos de este tipo de información las comunicaciones entre los altos directivos o accionistas con decisiones relevantes para la operativa de negocio.
Información Secreta	Es aquella información que únicamente debe conocer el propietario de la misma y no debe ser revelada bajo ningún concepto. La revelación o divulgación no autorizada de este tipo de información puede causar perjuicios excepcionalmente graves para los intereses esenciales de ACS Industrial.	Son ejemplos de este tipo de información las claves de acceso de colaboradores, credenciales de clientes o claves criptográficas para acceder a sistemas.