Norma de seguridad de la información para personal de empresas proveedoras

VERSIONADO

V1	Norma Inicial	10/11/2022
v2	Se corrigen alusiones a políticas, normas y requisitos	21/03/2024

ÍNDICE

1 Objetivo **3**
2 Alcance **3**
3 Responsabilidades **3**
4 Desarrollo **4**
4.1 Propósito y ámbito de aplicación 4
4.2 Seguridad en la prestación del servicio 4
4.2.1 Cumplimiento de la Política General de Seguridad del GRUPO AGBAR 4
4.2.2 Prestación de servicios a GRUPO AGBAR 5
4.2.3 Confidencialidad de la Información 5
4.2.4 Propiedad intelectual 6
4.2.5 Intercambio de información 7
4.2.6 Uso apropiado de los recursos 7
4.2.7 Uso apropiado de Internet 8
4.2.8 Uso apropiado del correo electrónico 9
4.2.9 Accesos privilegiados 10
4.2.10 Seguridad en desarrollo 10
4.2.11 Comunicación de incidencias 10
4.3 Seguridad en la prestación del servicio mediante el uso de la infraestructura del propio Proveedor 11
4.3.1 Seguridad de los activos 11
4.3.2 Gestión de identidades y accesos 11
4.3.3 Seguridad de sistemas 12
4.3.4 Seguridad de red 13
4.3.5 Seguridad de los equipos de usuario del Proveedor 14
4.3.6 Seguridad del Colaborador como usuario 14
5 Seguimiento y control **15**
6 Actualización de la Norma de Seguridad **16**

1 OBJETIVO

Con el fin de gestionar los riesgos asociados a los Sistemas de Información del GRUPO AGBAR, se establece la presente "Norma de Seguridad para personal de empresas proveedoras". En este documento se describen los requerimientos en relación a la seguridad de la información para todo el personal que trabaja para GRUPO AGBAR pero que pertenece a otras empresas proveedoras, y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de GRUPO AGBAR en general.

Las empresas proveedoras tienen la obligación de difundir convenientemente a las personas que destinen en GRUPO AGBAR, así como de obtener su compromiso por escrito de que se comprometen a respetar dichas Normas.

En función del lugar de la prestación del servicio, la propiedad de la infraestructura utilizada y la actividad a desarrollar, GRUPO AGBAR establece distintos requerimientos a cumplir por parte del proveedor.

La presente normativa tiene por objeto concretar la infraestructura utilizada para la prestación del servicio, indicar de manera detallada los controles obligatorios y otros elementos de los que se dota el proveedor para garantizar la seguridad física y del entorno.

2 ALCANCE

Esta norma se aplica a todos los empleados externos al GRUPO AGBAR que, en el desempeño de su trabajo utilizan activos, sistemas o infraestructura de la empresa para desarrollar los procesos de negocio.

3 RESPONSABILIDADES

El Responsable de Seguridad mantiene este documento, que es aprobado por la dirección y verifica la aplicación de las medidas de seguridad descritas en la norma.

El responsable del servicio del GRUPO AGBAR que proceda a una subcontratación parcial o total del servicio, se responsabiliza de comunicar al personal externo de la organización, contratistas y personal de terceras partes, según el caso, el presente documento, así como de recabar registro de aceptación por las mismas.

La alteración injustificada y no consensuada entre GRUPO AGBAR y el proveedor de los elementos que aquí se describen podrán considerarse, en función de la criticidad del servicio prestado y/o su reiteración, elementos suficientes para la adopción de las medidas sancionadoras que se consideren pertinentes en relación a la empresa contratada, y que pueden llegar a la resolución de los contratos que tenga vigentes con dicha empresa.

Este documento es propiedad del GRUPO AGBAR, y por lo tanto tiene carácter confidencial y únicamente está permitida su utilización y difusión con carácter interno a la empresa proveedora del servicio y por personal autorizado.

4 DESARROLLO

La infraestructura utilizada para la prestación del servicio constituye un elemento a tener en cuenta de cara a considerar el riesgo que supone para los activos del GRUPO AGBAR. La implantación de controles de seguridad sobre los elementos que intervienen recaerá, salvo que se indique lo contrario en la relación contractual, en el propietario de dicho activo.

La presente "Norma de Seguridad para personal de empresas proveedoras" establece de manera genérica los controles a implementar en función del elemento de que se trate. Dicha norma constituye norma de referencia para las posteriores revisiones y/o auditorías sobre los elementos indicados en el presente apartado.

4.1 Propósito y ámbito de aplicación

En toda organización existe información cuya pérdida o uso indebido puede dañar su reputación. Asimismo, el deterioro o indisponibilidad de los Sistemas de Información puede interrumpir el normal desarrollo de la operativa, produciendo efectos negativos en la calidad del servicio y los beneficios de la compañía.

El principal objetivo de este documento es establecer el marco normativo en relación a la seguridad de la información aplicable a los proveedores y colaboradores externos del Grupo AGBAR (en adelante los "Proveedores"), describiendo lo que se espera de todo el personal que trabaja para cualquiera de las empresas que forman parte del Grupo AGBAR pero que pertenece a otras empresas proveedoras o colaboradoras (en adelante los "Colaboradores"), y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información, recursos o activos del GRUPO AGBAR en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por el GRUPO AGBAR.

Para ello, los Proveedores se responsabilizan de informar de esta norma de seguridad los Colaboradores, así como de obtener su compromiso por escrito de que se comprometen a respetar dicha Política.

La Política de Seguridad refleja requerimientos legales y éticos, tanto en actuaciones informales de los Colaboradores, como en la realización de su operativa.

Con dicho propósito, esta norma contempla lo establecido en la Política de Seguridad del Grupo Agbar, y refleja las obligaciones a las que está sujeta por la legislación vigente, y en particular con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y todos sus desarrollos asociados.

4.2 Seguridad en la prestación del servicio

4.2.1 Cumplimiento de la Política General de Seguridad del GRUPO AGBAR

Todo Proveedor o Colaborador que desarrolle labores para el GRUPO AGBAR deberá tomar parte en el cumplimiento de la Política de Seguridad del Grupo, disponible en la web, y de la presente

norma de seguridad, observando sus directrices y colaborando en su aplicación dentro del ámbito de actuación de cada uno.

4.2.2 Prestación de servicios a GRUPO AGBAR

a) Los Proveedores sólo podrán desarrollar para el GRUPO AGBAR aquellas actividades cubiertas bajo el correspondiente pedido o contrato de prestación de servicios. De este modo, se entenderá que todas las actividades desarrolladas para el GRUPO AGBAR por los Colaboradores se encuadran en los pedidos o contratos de prestación de servicios que vinculan al GRUPO AGBAR con los Proveedores.
b) Las actividades desarrolladas por los Colaboradores se realizarán de acuerdo a lo establecido en el correspondiente pedido o contrato de prestación de servicios, así como a las normas y procedimientos establecidos a tal efecto entre el GRUPO AGBAR y el proveedor correspondiente.
c) El Proveedor proporcionará al GRUPO AGBAR periódicamente la relación de personas, perfiles, funciones y responsabilidades asociados al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
d) De acuerdo con lo establecido en las cláusulas asociadas al contrato de prestación de servicios, todo Colaborador que desarrolle labores para el GRUPO AGBAR deberá cumplir con los requisitos de seguridad recogidos en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones, el GRUPO AGBAR se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación tanto del Colaborador como del Proveedor.
e) El Proveedor deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio como de manera transversal en materia de seguridad de la información, para lo cual deberá asegurarse, al menos, de que todo el personal asociado al servicio conoce y se compromete a cumplir la presente Norma de Seguridad.
f) Cualquier tipo de intercambio de información que se produzca entre el GRUPO AGBAR y los Proveedores se entenderá que ha sido realizado dentro del marco establecido por el pedido o contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.
g) El Departamento de seguridad informática (SOC 360) centraliza los esfuerzos globales de protección de los activos del GRUPO AGBAR, a fin asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización.

4.2.3 Confidencialidad de la Información

a) Los Colaboradores que tengan acceso a información del GRUPO AGBAR deberán considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información del GRUPO AGBAR a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por parte del GRUPO AGBAR.
b) Los Colaboradores que presten servicios directamente en las instalaciones del GRUPO AGBAR, quedarán sometidos a las obligaciones de confidencialidad incluidas en el Acuerdo de Confidencialidad que el GRUPO AGBAR le remitirá al efecto, y que quedará vinculado a la presente Norma de Seguridad.

c) En cualquier caso, cualquier Colaborador, independientemente del lugar en el que preste los servicios, quedará sometido a las obligaciones de confidencialidad contenidas en la presente Norma de Seguridad, a saber:
    - Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en que se encuentre contenida.
    - Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior información confidencial, salvo que esté debidamente autorizado.
    - Se minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
    - Ningún colaborador en proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada al GRUPO AGBAR.
    - En el caso de que, por motivos directamente relacionados con la prestación de los servicios, el Colaborador entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Asimismo, el Colaborador deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación entre el GRUPO AGBAR y el Proveedor. La utilización continuada de la información confidencial en cualquier formato o soporte distinta a la pactada y sin conocimiento del GRUPO AGBAR no supondrá, en ningún caso, una modificación de este punto.
    - Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el Colaborador desarrolle para el GRUPO AGBAR.
    - El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo 197 del Código Penal, que puede dar derecho a exigir compensaciones.

d) Para garantizar la seguridad de los Datos de Carácter Personal los Proveedores y Colaboradores deberán observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:
    - El Colaborador sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades externas USB del Colaborador y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
    - No se albergarán datos de carácter personal en las unidades externas USB.
    - La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable del fichero y se realizará según el procedimiento definido.
    - Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

4.2.4 Propiedad intelectual

a) Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

b) Los Colaboradores únicamente podrán utilizar material autorizado por el GRUPO AGBAR para el desarrollo de sus funciones.
c) Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia.
d) Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.
e) El GRUPO AGBAR únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

4.2.5 Intercambio de información

a) Ninguna persona debe ocultar o manipular su identidad en ninguna circunstancia.
b) La distribución de información ya sea en formato digital o papel se realizará para la finalidad exclusiva de facilitar las funciones asociadas al contrato de prestación de servicios. El GRUPO AGBAR se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos recursos de difusión.
c) En relación al intercambio de información dentro del marco del contrato de prestación de servicios, se considerarán no autorizadas las siguientes actividades:
    - Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
    - Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
    - Transferencia de ficheros a terceras partes no autorizadas de material del GRUPO AGBAR o material que es de alguna u otra manera confidencial.
    - Transmisión o recepción de ficheros que infrinjan la legislación vigente en materia de Protección de Datos de Carácter Personal o directrices del GRUPO AGBAR.
    - Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
    - Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con el servicio a prestar por parte del Proveedor.
    - Todas las actividades que puedan dañar la buena reputación del GRUPO AGBAR están prohibidas en Internet y en cualquier otro lugar.

4.2.6 Uso apropiado de los recursos

a) El Proveedor se compromete a informar periódicamente al GRUPO AGBAR de los activos con los que proporciona el servicio.
b) El Proveedor se compromete a utilizar los recursos dispuestos para la provisión del servicio de acuerdo con las condiciones para las que fueron diseñados e implantados.
c) Los recursos que el GRUPO AGBAR pone a disposición de los Colaboradores, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para el que fueron proporcionados. El GRUPO AGBAR se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

d) Todos los equipos del Proveedor que se conecten a la red del GRUPO AGBAR deberán cumplir los requisitos técnicos definidos por el GRUPO[1]. El proveedor pondrá a disposición del GRUPO AGBAR dichos equipos para que, si fuera necesario para el desarrollo de los trabajos contratados, el GRUPO AGBAR les instale el software homologado y los configure apropiadamente.
e) Se deberán restituir al GRUPO AGBAR todos los activos físicos y destruir o restituir al GRUPO AGBAR todos los activos de información, sin retraso injustificado, después de la finalización del contrato de prestación de Servicios entre el GRUPO AGBAR y el Proveedor.
f) Se prohíbe expresamente:
    - El uso de los recursos proporcionados por el GRUPO AGBAR para actividades no relacionadas con el propósito del servicio.
    - La conexión a la red de producción del GRUPO AGBAR de equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios del GRUPO AGBAR o bajo supervisión del GRUPO AGBAR.
    - Introducir voluntariamente en la red del GRUPO AGBAR cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todo Colaborador con acceso a la red del GRUPO AGBAR tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
    - Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que el GRUPO AGBAR les haya asignado.
    - Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de Información del GRUPO AGBAR.
    - Intentar distorsionar o falsear los registros “log” de los Sistemas de Información del GRUPO AGBAR.
    - Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos del GRUPO AGBAR.
    - Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los Recursos Informáticos del GRUPO AGBAR.
    - Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos responsabilidad del GRUPO AGBAR (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
    - Albergar datos de carácter personal del GRUPO AGBAR o cuyo tratamiento haya sido encomendado al GRUPO AGBAR en las unidades locales de disco de los puestos PC de usuario.

4.2.7 Uso apropiado de Internet

Siempre que se haga uso del acceso a Internet proporcionado por el GRUPO AGBAR se deberán respetar, adicionalmente, los siguientes requisitos:

a) Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Los usuarios no deben buscar o visitar sitios que no sirvan como soporte al objetivo de negocio del GRUPO AGBAR o al cumplimiento de su trabajo diario.

[1] Véase “Requerimientos técnicos de los dispositivos informáticos de los colaboradores externos”

b) El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporados en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.
c) Los usuarios no deberán usar el nombre, símbolo, logotipo o símbolos similares al del GRUPO AGBAR en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
d) Únicamente se permitirá la transferencia de datos de o hacia Internet cuando estén relacionadas con actividades del negocio. La transferencia de ficheros no relativa a estas actividades (por ejemplo, la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia, etc.) estarán prohibidas.

4.2.8 Uso apropiado del correo electrónico

Siempre que se haga uso de una cuenta de correo electrónico proporcionado por el GRUPO AGBAR se deberán respetar, adicionalmente, las siguientes requisitos:

a) Aunque el uso personal no está prohibido, éste debe restringirse al mínimo necesario, y en ningún caso debe interferir con el desempeño de tus tareas. Adicionalmente, no se debe:
    - Enviar archivos adjuntos de gran tamaño, incluyendo juegos, imágenes, ficheros ejecutables, videos.
    - Crear, enviar o recibir mensajes en cadena con salvapantallas o presentaciones lúdicas,
    - Utilizar el identificador de otro usuario para enviar correo electrónico,
    - Enviar cualquier comunicación personal de carácter privado que no quieres que otra persona pueda ver.
    - Utilizar software de mensajería instantánea que no haya sido aprobado por la empresa.
b) No se debe escribir o enviar nada por correo electrónico que pueda dañar la imagen de la empresa.
c) En ningún caso se debe utilizar la comunicación electrónica para enviar, almacenar, reenviar o transmitir de ninguna manera el material descrito a continuación:
    - Material que viole las obligaciones de confidencialidad para con la empresa o cualquier otra tercera parte interesada, o que viole las leyes de propiedad intelectual, copyright, u otras aplicables.
    - Material difamatorio, ofensivo, vulgar u obsceno (incluyendo cualquier tipo de pornografía),
    - Cualquier material falso o malicioso, tanto de algún empleado/a de la empresa como de otra persona,
    - Material sexista o racista,
    - Cualquier otro material que pueda considerarse ilegal o que sea susceptible de formar parte de las categorías anteriores.
    - Leer, grabar, copiar o escuchar cualquier mensaje o información enviada a otro usuario sin el permiso de éste.
d) El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos

4.2.9 Accesos privilegiados

Todos los Proveedores que dispongan de acceso privilegiado a los sistemas de información del GRUPO AGBAR deberán cumplir los siguientes requisitos de selección:

a) El Proveedor deberá verificar los antecedentes profesionales del Colaborador asignado al servicio, garantizando al GRUPO AGBAR que en el pasado no ha sido sancionado por mala praxis profesional ni se ha visto envuelto en incidentes relacionados con la confidencialidad de la información tratada que le hayan supuesto algún tipo de sanción.
b) El Proveedor garantiza, en el caso de baja de un Colaborador, la inmediata comunicación al departamento correspondiente del GRUPO AGBAR para que procedan al bloqueo del mismo de forma inmediata.

4.2.10 Seguridad en desarrollo

Todos los Proveedores que dispongan de acceso (tanto privilegiado como no privilegiado) a los sistemas de información del GRUPO AGBAR y que realicen actividades de desarrollo de aplicativos deberán garantizar que se cumplen, al menos, los siguientes requisitos de seguridad en dicha actividad:

a) Todo el proceso de desarrollo de software externalizado será controlado y supervisado por del GRUPO AGBAR, y se desarrollará de acuerdo con un proceso formal que determine las reglas a seguir.
b) Se incorporarán mecanismos de identificación, autenticación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implementación y operación de los aplicativos.
c) Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.
d) Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.
e) Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.
f) Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
g) Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.
h) El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.
i) Durante las fases de desarrollo y pruebas se llevarán a cabo pruebas específicas de las funcionalidades de seguridad.
j) En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.
k) Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.
l) Sólo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

4.2.11 Comunicación de incidencias

Todo Proveedor y/o Colabrador que tenga utilice o tenga acceso a los sistemas de información del GRUPO AGBAR, independientemente del lugar en el que preste sus servicios, deberá, en el caso de

que detecte cualquier incidencia relacionada con la información o con los recursos del GRUPO AGBAR puestos a su disposición, así como cualquier vulnerabilidad o situacion de riesgo que pueda tener relación con la seguridad de la información o con las directrices contempladas en las presentes políticas, ponerse en contacto con el ServiceDesk a través del Chat HelpDesk https://cauagbar-is.onbmc.com/com.bmc.dsm.chatbot/index.html o bien telefónicamente (93 342 25 23/ 902 12 06 13).

4.3 Seguridad en la prestación del servicio mediante el uso de la infraestructura del propio Proveedor

4.3.1 Seguridad de los activos

Todos los Proveedores que presten servicio mediante el uso de infraestructura propia del Proveedor deberán garantizar que se cumplen, al menos, los siguientes requisitos de gestión de activos:

a) El Proveedor deberá contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.
b) Todos los activos utilizados para la prestación del servicio deberán tener un responsable, que deberá asegurarse que dichos activos incorporan las medidas de seguridad mínimas establecidas por la organización, y que al menos deben ser las especificadas en la presente norma.
c) El Proveedor deberá notificar al GRUPO AGBAR las bajas de los activos utilizados para la prestación del servicio. Si dicho activo contiene otra propiedad del GRUPO AGBAR (hardware, software u otro tipo de activos), deberá ser entregado previamente a llevar a cabo la baja para que el GRUPO AGBAR proceda a la retirada de los activos de su propiedad.
d) Siempre que un activo haya contenido información responsabilidad del GRUPO AGBAR, el proveedor deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable.

4.3.2 Gestión de identidades y accesos

Todos los Proveedores que presten servicio al GRUPO AGBAR mediante el uso de la infraestructura del propio proveedor deberán garantizar que se cumplen, al menos, las siguientes requisitos de control y gestión de identidades y accesos a la hora de acceder a información del GRUPO AGBAR:

a) Todos los usuarios con acceso a un sistema de información dispondrán de una autorización de acceso unipersonal compuesta de identificador de usuario y contraseña. Esta obligación deberá ser cumplida tanto por todos los usuarios y especialmente por los usuarios con privilegios de administración de dichos sistemas de información.
b) Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
c) Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
d) Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
e) La longitud mínima de la contraseña deberá ser de 8 caracteres.

f) Las contraseñas estarán constituidas por combinación de caracteres alfanuméricos y especiales, incluyendo al menos un carácter numérico, una letra mayúscula, una letra minúscula y un carácter especial.
g) Es recomendable utilizar las siguientes directrices para la selección de contraseñas:
    - No usar palabras conocidas, ni palabras que se puedan asociar con uno mismo, por ejemplo, el nombre.
    - La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc.
    - La clave debería ser algo prácticamente imposible de adivinar. Pero al mismo tiempo debería ser fácilmente recordada por el usuario. Un buen ejemplo es usar el acrónimo de alguna frase o expresión.
    - La clave debería contener al menos un carácter numérico y uno alfabético.
    - La clave no debería empezar ni acabar con un carácter numérico.
    - No se debería utilizar el identificador de usuario como parte de la clave secreta.
h) El proveedor deberá garantizar que periódicamente se constata que sólo tienen acceso a la información responsabilidad del GRUPO AGBAR el personal debidamente autorizado para ello (revisión de los derecho de acceso).
i) Siempre que sea posible el acceso a los sistemas de información requerirán que el usuario tenga habilitada la doble autenticación.
j) En aquellos casos en los que además se acceda a los sistemas de información del GRUPO AGBAR se deberán considerar, además, los siguientes requisitos adicionales:
    - Ningún usuario recibirá un identificador de acceso a los sistemas del GRUPO AGBAR hasta que no acepte formalmente la Norma de Seguridad vigente.
    - Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
    - En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 90 días. En caso contrario, se le podrá denegar el acceso y deberá contactar con el ServiceDesk para la obtención de una nueva.
    - Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
    - En relación con datos de carácter personal, exclusivamente el personal autorizado para ello podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.
    - Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y con el ServiceDesk para notificar la incidencia.

4.3.3 Seguridad de sistemas

Todos los Proveedores que presten servicio al GRUPO AGBAR mediante el uso de la infraestructura del propio proveedor deberán garantizar que se cumplen, al menos, los siguientes requisitos de seguridad de sistemas:

a) Los sistemas de información que alberguen o traten información del GRUPO AGBAR deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la política de backup de la organización.
b) Los relojes de los sistemas del Proveedor que procesen o alberguen información del GRUPO AGBAR estarán sincronizados entre sí y con la hora oficial (servidor ntp).

c) El Proveedor del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información del GRUPO AGBAR se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.
d) Los sistemas de información que alberguen o procesen información del GRUPO AGBAR estarán adecuadamente protegidos frente a software malicioso, aplicando las siguientes precauciones:
    - Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de prueba, desarrollo y producción.
    - El software antivirus o, en su defecto, el software Endpoint Detection and Response se deberá instalar y usar en todos los servidores y ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
    - El software antivirus o, en su defecto, el software Endpoint Detection and Response deberá estar siempre habilitado. Se establecerá una actualización automática, de los ficheros de definición de virus tanto en los ordenadores personales como servidores, así como de bloqueo frente a la detección de virus informáticos.
e) El Proveedor establecerá una política de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad máxima mensual.
f) Siempre que se utilice el correo electrónico en relación con el servicio prestado, el proveedor deberá respetar las siguientes premisas:
    - No se permitirá la transmisión vía correo electrónico de información confidencial del GRUPO AGBAR salvo que la comunicación electrónica esté cifrada y el envío esté expresamente permitido.
    - No se permitirá la transmisión vía correo electrónico de información que contenga datos de carácter personal de carácter sensible, salvo que la comunicación electrónica esté cifrada y el envío esté expresamente permitido.
g) Siempre que se haga uso de software facilitado por del GRUPO AGBAR, en la infraestructura del Prestador, se deberán atender los siguientes requisitos:
    - Todo Colaborador que acceda a los Sistemas de Información puesto a su disposición debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
    - Todo Colaborador tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

4.3.4 Seguridad de red

Todos los Proveedores que presten servicio al GRUPO AGBAR mediante el uso de la infraestructura del propio proveedor deberán garantizar que se cumplen, al menos, los siguientes requisitos de seguridad de red:

a) Las redes a través de las que circule la información del GRUPO AGBAR deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por el proveedor.
b) Las redes que permitan el acceso a la infraestructura del GRUPO AGBAR deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:
    - El acceso de usuarios remotos a la red del GRUPO AGBAR estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso.

- Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales (VPN) o líneas dedicadas.
- En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones que posibilite conexiones alternativas no controladas.

c) El acceso a las redes a través de las que circule la información responsabilidad del GRUPO AGBAR deberá estar limitado.

d) Todos los equipos conectados a las redes a través de las que circule la información responsabilidad del GRUPO AGBAR deberán estar apropiadamente identificados, de modo que los tráficos de red puedan ser identificables.

e) El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la aplicación de los siguientes requisitos:
    - Se establecerán criterios de autorización del teletrabajo en base a las necesidades del puesto de trabajo.
    - Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
    - Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
    - Se controlará la revocación de derechos de acceso y devolución de equipamiento tras la finalización del periodo de necesidad del mismo.

4.3.5 Seguridad de los equipos de usuario del Proveedor

a) Todos los equipos de usuario estarán adecuadamente protegidos frente a malware:
    - El software antivirus se deberá instalar y usar en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
    - Se mantendrán al día con las últimas actualizaciones de seguridad disponibles.
    - El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los ficheros de definición de virus.
    - El usuario no dispondrá de capacidad para deshabilitar el software antivirus.

b) Se velará especialmente por la seguridad de todos los equipos móviles de usuario que contengan información del GRUPO AGBAR o permitan acceder a ella de algún modo:
    - Verificando que no incluyen más información del GRUPO AGBAR que la que sea estrictamente necesaria.
    - Garantizando que se aplican controles de acceso a dicha información.
    - Minimizando los accesos a dicha información en presencia de personas ajenas al servicio provisto al GRUPO AGBAR.
    - Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a golpes.
    - Tomando especiales precauciones en el exterior de las dependencias del GRUPO AGBAR para evitar la visión accidental por parte de terceras personas de la información del GRUPO AGBAR mediante, por ejemplo, el uso de filtros de privacidad en pantallas.

4.3.6 Seguridad del Colaborador como usuario

a) Los Proveedores deberán asegurarse de que todo Colaborador respete los siguientes principios básicos dentro de su actividad informática:
    - Cada persona con acceso a información del GRUPO AGBAR es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control

los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto de Colaboradores ni personal del GRUPO AGBAR bajo ningún concepto.
    - Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del GRUPO AGBAR.

b) Cualquier persona con acceso a información del GRUPO AGBAR deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos, activando su bloqueo.

c) Cualquier persona con acceso a información del GRUPO AGBAR deberá respetar al menos los siguientes requisitos de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
    - Almacenar bajo llave los documentos en papel y los medios informáticos con información del GRUPO AGBAR en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
    - No dejar desatendidos los equipos asignados a funciones del GRUPO AGBAR, y bloquear su acceso cuando se ausente el usuario.
    - Proteger, siempre que se utilice información del GRUPO AGBAR, tanto los puntos de recepción y envío de información (correo postal, scanner) como los equipos de duplicado (fotocopiadora y scanner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad del usuario.
    - Retirar, sin retraso injustificado, cualquier información confidencial que sea del GRUPO AGBAR, una vez impresa.
    - Los listados con datos de carácter personal o información confidencial del GRUPO AGBAR deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
    - Los listados con datos de carácter personal o información confidencial del GRUPO AGBAR deberán eliminarse de manera segura una vez no sean necesarios.
    - Las personas con acceso a sistemas y/o información del GRUPO AGBAR nunca deberán sin autorización explícita, realizar pruebas para detectar y/o utilizar una supuesta debilidad o incidente de seguridad, en caso de identificarse incidentes o debilidades que puedan suponerse relacionadas con la seguridad de la información.
    - Ninguna persona con acceso a sistemas y/o información del GRUPO AGBAR intentará sin autorización explícita por ningún medio transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas.

5 SEGUIMIENTO Y CONTROL

Con el fin de velar por el correcto uso de los recursos informáticos mencionados en el presente documento, a través de los mecanismos formales y técnicos que se considere oportunos, el GRUPO AGBAR comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, la correcta utilización de dichos recursos por todos los Colaboradores así como el cumplimiento de lo descrito en la presente norma.

En caso de apreciar que alguien utiliza incorrectamente los recursos, la información confidencial, datos personales, aplicaciones y/o cualquier otro dato, principalmente, así como cualquier otro recurso informático, se le comunicará tal circunstancia y se le facilitará, en su caso, la formación necesaria para el correcto uso de los recursos.

En caso de apreciarse mala fe en la incorrecta utilización de las aplicaciones y/o datos, principalmente, así como cualquier otro recurso informático, el GRUPO AGBAR ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6 Actualización de la Norma de Seguridad

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, el GRUPO AGBAR se reserva el derecho a modificar la presente Norma de Seguridad para personal de empresas proveedoras cuando sea necesario.

Los cambios realizados en la presente norma serán divulgados a los Proveedores y en su caso, Colaboradores a las que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada Proveedor garantizar la lectura y conocimiento del presente documento, en su versión más actualizada, por parte de cada Colaborador.