BASF Group –
Cyber Security Addendum

Versión	**5.1**
Clasificación	**P U B L I C**

Detalles de la versión

Versión	5.1
Creado por	Sebastian Krüsmann, NeoMINT GmbH
Estado	Aprobado
Aprobado el	10.01.2024
Aprobado por	Julia Mansky, BASF Digital Solutions GmbH
Actualizaciones en	Download Center (basf.com)

Historia

Versión	Fecha	Creado por	Cambios
1.0	02.10.2023	Sebastian Krüsmann, NeoMINT GmbH	Creación inicial
2.0	09.10.2023	Sebastian Krüsmann, NeoMINT GmbH	Cambios editoriales
3.0	17.10.2023	Sebastian Krüsmann, NeoMINT GmbH	Cambios editoriales
4.0	21.11.2023	Sebastian Krüsmann, NeoMINT GmbH	Cambios editoriales
5.0	08.01.2024	Sebastian Krüsmann, NeoMINT GmbH	Cambios editoriales
5.1	08.08.2024	Beatrice Huck, NeoMint GmbH	Adición de control C-T-12 y S-T-12, CL-T-15 Cambio de control C-T-13, S-T-13 CL-T-16, CL-T-09, C-T-06 y S-T-06

Índice

1 Descargo de responsabilidad

El apéndice de seguridad contiene requisitos para la seguridad de la información.

Todos los proveedores de TI deben cumplir las especificaciones del capítulo "Generalidades". Los **demás requisitos** están **separados según el tipo de proveedor** y deben cumplirse en consecuencia. Encontrará una explicación de los tipos de proveedores al principio del capítulo correspondiente.

Para cada tipo de proveedor, hay capítulos en los que se describen los riesgos específicos y el objetivo que debe alcanzarse abordando el riesgo. Para ello, existen diversas medidas de carácter técnico u organizativo que pueden aplicarse normalmente. En caso de que el riesgo no sea relevante para un caso concreto o de que un proveedor opine que un riesgo podría abordarse de forma diferente a la indicada, existe la posibilidad de explicarlo brevemente. Corresponde a BASF decidir si las razones y medidas dadas son suficientes.

2 Puntos de contacto para la ciberseguridad

Con el fin de garantizar una cooperación fluida y eficaz con nuestros proveedores de TI para mantener un nivel adecuado de ciberseguridad, cada proveedor debe designar personas de contacto e información de contacto para las principales funciones de ciberseguridad.

El cliente interno (iBP o Compras) documenta la información en el formulario *2 IT-Supplier Security Assessment_EN_Contact Sheet* en la versión actual en alemán o inglés para cada proveedor y la envía al equipo de seguridad de proveedores.

3 General

La seguridad general del proveedor es relevante si los riesgos se aplican independientemente del servicio prestado.

3.1 (Punto de contacto (único) para ciberseguridad / seguridad de la información

Riesgo abordado Una comunicación inadecuada o tardía con los proveedores sobre cuestiones de ciberseguridad podría dar lugar a que las vulnerabilidades se aborden tarde o de forma inadecuada.

Objetivo Las consultas sobre cuestiones de ciberseguridad, por ejemplo, sobre las medidas de seguridad aplicadas o en caso de descubrimiento de incidentes de seguridad que afecten al proveedor, se responderán en un plazo razonable.

Medidas técnicas	
G-T-01	Plataforma a través de la cual se envían las consultas y se responde con prontitud, por ejemplo, sistema de tickets.

Medidas organizativas	
G-O-01	Punto de contacto para cuestiones de ciberseguridad, por ejemplo, CISO / Responsable de Seguridad de la Información.

3.2 Recursos humanos Seguridad

Riesgo abordado Los empleados de los proveedores podrían tener un impacto negativo significativo en el nivel de seguridad de BASF a través de su comportamiento, tanto intencionadamente como por descuido.

Objetivo Sólo se permite el acceso a la información o a los sistemas de BASF a empleados suficientemente cualificados y concienciados.

Medidas técnicas	
G-T-02	Concepto de función y autorización: Los empleados sólo tienen acceso a la información relevante para su trabajo (principio de necesidad de conocer).

Medida organizativa	
G-O-02	Formación periódica sobre ciberseguridad para todos los empleados

3.3 Gestión de la seguridad de la información

Riesgo abordado Una conceptualización y operacionalización insuficientes de la ciberseguridad podría dar lugar a que las vulnerabilidades no se identificaran o evitaran en una fase temprana. La explotación de dichas vulnerabilidades por un atacante podría tener un impacto negativo en el nivel de seguridad de BASF.

Objetivo Diseño y gestión proactivos de la totalidad de los mecanismos de seguridad del proveedor.

Medidas organizativas	
G-O-03	Designación de una persona responsable de mantener un nivel adecuado de ciberseguridad, por ejemplo, CISO o responsable de seguridad de la información.
G-O-04	Gestión de la totalidad de las medidas de ciberseguridad en el ámbito de un sistema de gestión de la seguridad de la información (SGSI)
G-O-05	Certificación del sistema de gestión de la seguridad de la información basada en una norma establecida, por ejemplo ISO 27001

3.4 Seguridad de la cadena de suministro

Riesgo abordado Una conceptualización y operacionalización insuficientes de la ciberseguridad podría dar lugar a que las vulnerabilidades no se identificaran o evitaran en una fase temprana. La explotación de dichas vulnerabilidades por un atacante podría tener un impacto negativo en el nivel de seguridad de BASF.

Objetivo Exigir a todos los subcontratistas y proveedores de materiales que establezcan y mantengan un nivel adecuado de ciberseguridad.

Medidas organizativas	
G-O-06	Registro de subproveedores contratados para la prestación de servicios a BASF
G-O-07	Obligación contractual de los subcontratistas y proveedores de establecer y mantener un nivel adecuado de ciberseguridad.

3.5 Gestión del cambio

Riesgo abordado Un control inadecuado de los cambios en los servicios y productos prestados podría dar lugar a pérdidas de información y a la degradación del rendimiento, lo que podría repercutir negativamente en las operaciones de BASF.

Objetivo Establecer un procedimiento normalizado y formalizado para coordinar y comprometerse con los cambios de los servicios y productos prestados.

Medidas técnicas	
G-T-03	Plataforma a través de la cual se gestionan y documentan todos los cambios de contratos y servicios.

Medidas organizativas	
G-O-08	(Punto de contacto (único) para cambios en los servicios contratados

3.6 Conformidad

Abordado el riesgo de que BASF pueda ser considerada responsable de infracciones de leyes y reglamentos causadas por los proveedores.

Objetivo Se respetan en todo momento todos los requisitos de cumplimiento aplicables.

Medidas organizativas	
G-O-09	Designación de una persona responsable de mantener el cumplimiento global, por ejemplo, un responsable de cumplimiento.
G-O-10	Gestión de todas las medidas de cumplimiento en el ámbito de un sistema de gestión del cumplimiento (SGC)

4 Servicios de consultoría

Todos los servicios de consultoría relacionados directa o indirectamente con el desarrollo organizativo, así como el suministro, funcionamiento o desmantelamiento de soluciones informáticas.

4.1 Gestión de recursos

Riesgo abordado La escasez de personal podría hacer que no se prestaran los servicios acordados contractualmente.

Objetivo Se garantiza en todo momento la disponibilidad de empleados suficientemente cualificados para la prestación de los servicios acordados contractualmente. Todos los servicios pueden prestarse a tiempo y con la calidad acordada.

Medidas organizativas	
C-O-01	Gestión de los recursos humanos en el ámbito de la gestión interna de recursos para proporcionar personal cualificado
C-O-02	Concepto de formación y desarrollo para el personal especializado y directivo

4.2 Tratamiento de la información

Riesgo abordado La información utilizada en los proyectos de consultoría podría comprometer la ciberseguridad de BASF si se pierde la confidencialidad.

Objetivo Se garantiza en todo momento que toda la información creada y recibida en el ámbito de los proyectos de consultoría se trata de forma confidencial y se protege para que no se vea comprometida.

Medidas técnicas	
C-T-01	Cifrado de la comunicación por correo electrónico mediante una norma establecida del sector, por ejemplo, PGP, S/MIME
C-T-02	Cifrado de discos duros de dispositivos móviles, por ejemplo, BitLocker, Vera Crypt
C-T-03	Cifrado de discos duros de servidores, por ejemplo, BitLocker, Vera Crypt

C-T-04	Cifrado de soportes de datos móviles, por ejemplo, BitLocker, Vera Crypt, cifrado de hardware
C-T-05	Gestión de todos los permisos en el ámbito de la gestión integral de identidades y accesos (IAM)

Medidas organizativas

C-O-03	Política de almacenamiento, tratamiento y envío de información antes, durante y después de los proyectos
C-O-04	Proceso de gestión de incidentes de seguridad
C-O-05	Proceso de borrado remoto de datos en caso de pérdida de dispositivos móviles
C-O-06	Proceso para garantizar que sólo los empleados que prestan servicios de consultoría para BASF tienen acceso a la información de BASF (principio de necesidad de conocer).
C-O-07	Proceso de concesión, modificación o revocación de derechos de acceso cuando los empleados se incorporan o abandonan la empresa o cambian de función (proceso Joiner-Mover-Leaver).
C-O-08	Concepto de clasificación de la información procesada en función de su criticidad

4.3 Protección contra malware

Riesgo abordado Si los dispositivos informáticos utilizados en el proceso de consultoría se ven comprometidos, la información podría modificarse involuntariamente o hacerse accesible a terceros no autorizados.

Objetivo Se garantiza que no puedan instalarse programas maliciosos en los dispositivos informáticos.

Medidas técnicas	
C-T-06	Solución de protección contra malware para servidores Windows
C-T-07	Solución de protección contra malware en clientes, por ejemplo, Microsoft Defender
C-T-08	Dispositivos de seguridad, por ejemplo, cortafuegos, SIEM
C-T-09	Segmentación adecuada de la red corporativa basada en la criticidad con respecto a los requisitos de confidencialidad y disponibilidad de los datos procesados.
C-T-10	Uso de una solución sandbox para abrir archivos desconocidos o de remitentes desconocidos.
C-T-11	Distribución de software gestionada centralmente
C-T-12	No concesión de derechos de administración local a los promotores
C-T-13	No se conceden derechos de administración local a los usuarios habituales

Medidas organizativas	
C-O-09	Proceso para la instalación inmediata de actualizaciones relevantes para la seguridad de todas las soluciones de software en uso.
C-O-10	Política de refuerzo de servidores
C-O-11	Política de endurecimiento para clientes
C-O-12	Política de endurecimiento para smartphones

4.4 Copia de seguridad de datos

Riesgo abordado Los errores del sistema, los programas maliciosos o el uso indebido de los sistemas informáticos podrían provocar la pérdida de los datos recopilados en el marco de un proyecto de consultoría.

Objetivo Se realizan copias de seguridad periódicas de todos los datos relevantes para BASF, que pueden restaurarse en caso de pérdida de datos.

Medidas técnicas	
C-T-14	Copias de seguridad periódicas y automatizadas de todos los datos relevantes para BASF.

Medidas organizativas	
C-O-13	Concepto de copia de seguridad
C-O-14	Ejercicios regulares de copia de seguridad y recuperación de datos

4.5 Seguridad física

Riesgo abordado Al ser procesada en las instalaciones del proveedor, la información de BASF podría verse comprometida por partes externas.

Goal Toda la información de y sobre BASF está protegida contra el acceso físico de terceros no autorizados.

Medidas técnicas	
C-T-15	Oficinas con cerradura
C-T-16	Armarios con cerradura o cajas fuertes

Medidas organizativas	
C-O-15	Política de acompañamiento de invitados en las propiedades del proveedor por parte de los empleados
C-O-16	Política de bloqueo de soportes de almacenamiento de datos, equipos informáticos y documentos

4.6 Protección de la información personal identificable (IPI)

Riesgo abordado Cuando se procesan datos de identificación personal en el ámbito del tratamiento contratado, los derechos personales de los interesados podrían verse comprometidos por un uso inadecuado de la información.

Objetivo Al procesar la IIP, se garantiza en todo momento que se cumplen los requisitos del GDPR y las normativas de protección de datos posteriores.

Medidas organizativas	
C-O-17	Designación de una persona responsable de la protección de datos, por ejemplo, un responsable de la protección de datos
C-O-18	Protección de la totalidad de la información personal identificable en el ámbito de un sistema de gestión de la protección de datos (SGD)

5 Servicio y asistencia

Todos los servicios de servicio y asistencia en cuyo ámbito se administran, mantienen o eliminan las soluciones. Abarca todo el ciclo de vida de una solución, desde su instalación hasta su eliminación.

5.1 Gestión de recursos

Riesgo abordado La escasez de personal podría hacer que no se prestaran los servicios acordados contractualmente.

Objetivo Se garantiza en todo momento la disponibilidad de empleados suficientemente cualificados para la prestación de los servicios acordados contractualmente. Todos los servicios pueden prestarse a tiempo y con la calidad acordada.

Medidas organizativas	
S-O-01	Gestión de los recursos humanos en el ámbito de la gestión interna de recursos para proporcionar personal cualificado
S-O-02	Concepto de formación y desarrollo para el personal especializado y directivo

5.2 Tratamiento de la información

Riesgo abordado La información utilizada en los servicios y tareas de apoyo podría comprometer la ciberseguridad de BASF si se pierde la confidencialidad.

Objetivo Se garantiza en todo momento que toda la información creada y recibida en el ámbito de los servicios y actividades de apoyo se trata confidencialmente y se protege para que no se vea comprometida.

Medidas técnicas	
S-T-01	Cifrado de la comunicación por correo electrónico mediante una norma establecida del sector, por ejemplo, PGP, S/MIME
S-T-02	Cifrado de discos duros de dispositivos móviles, por ejemplo, BitLocker, Vera Crypt
S-T-03	Cifrado de discos duros de servidores, por ejemplo, BitLocker, Vera Crypt
S-T-04	Cifrado de soportes de datos móviles, por ejemplo, BitLocker, Vera Crypt, cifrado de hardware
S-T-05	Gestión de todos los permisos en el ámbito de la gestión integral de identidades y accesos (IAM)
Medidas organizativas	
S-O-03	Política de almacenamiento, tratamiento y envío de información antes, durante y después de las misiones
S-O-04	Proceso de gestión de incidentes de seguridad
S-O-05	Proceso de borrado remoto de datos en caso de pérdida de dispositivos móviles
S-O-06	Proceso para garantizar que sólo los empleados que prestan servicios de consultoría para BASF tienen acceso a la información de BASF (principio de necesidad de conocer).
S-O-07	Proceso de concesión, modificación o revocación de derechos de acceso cuando los empleados se incorporan o abandonan la empresa o cambian de función (proceso Joiner-Mover-Leaver).

S-O-08	Concepto de clasificación de la información procesada en función de su criticidad

5.3 Protección contra malware

Riesgo abordado Si los dispositivos informáticos utilizados en los servicios y tareas de apoyo se ven comprometidos, la información podría modificarse involuntariamente o quedar accesible a terceros no autorizados.

Objetivo Se garantiza que no puedan instalarse programas maliciosos en los dispositivos informáticos.

Medidas técnicas	
S-T-06	Solución de protección contra malware para servidores Windows
S-T-07	Solución de protección contra malware en clientes, por ejemplo, Microsoft Defender
S-T-08	Dispositivos de seguridad, por ejemplo, cortafuegos, SIEM
S-T-09	Segmentación adecuada de la red corporativa basada en la criticidad con respecto a los requisitos de confidencialidad y disponibilidad de los datos procesados.
S-T-10	Uso de una solución sandbox para abrir archivos desconocidos o de remitentes desconocidos.
S-T-11	Distribución de software gestionada centralmente
S-T-12	No concesión de derechos de administración local a los promotores
S-T-13	No se conceden derechos de administración local a los usuarios habituales

Medidas organizativas	
S-O-09	Proceso para la instalación inmediata de actualizaciones relevantes para la seguridad de todas las soluciones de software en uso.
S-O-10	Política de refuerzo de servidores
S-O-11	Política de endurecimiento para clientes
S-O-12	Política de endurecimiento para smartphones

5.4 Copia de seguridad de datos

Riesgo abordado Los errores del sistema, el malware o el uso indebido de los sistemas informáticos podrían provocar la pérdida de datos relevantes para BASF.

Objetivo Se realizan copias de seguridad periódicas de todos los datos relevantes para BASF, que pueden restaurarse en caso de pérdida de datos.

Medidas técnicas	
S-T-14	Copias de seguridad periódicas y automatizadas de todos los datos relevantes para BASF.

Medidas organizativas	
S-O-13	Concepto de copia de seguridad
S-O-14	Ejercicios regulares de copia de seguridad y recuperación de datos

5.5 Seguridad física

Riesgo abordado Al ser procesada en las instalaciones del proveedor, la información de BASF podría verse comprometida por partes externas.

Goal Toda la información de y sobre BASF está protegida contra el acceso físico de terceros no autorizados.

Medidas técnicas	
S-T-15	Oficinas con cerradura
S-T-16	Armarios con cerradura o cajas fuertes

Medidas organizativas	
S-O-15	Política de acompañamiento de invitados en las propiedades del proveedor por parte de los empleados
S-O-16	Política de bloqueo de soportes de almacenamiento de datos, equipos informáticos y documentos

5.6 Protección de la información personal identificable (IPI)

Riesgo abordado Cuando se procesan datos de identificación personal en el ámbito del tratamiento contratado, los derechos personales de los interesados podrían verse comprometidos por un uso inadecuado de la información.

Objetivo Al procesar la IIP, se garantiza en todo momento que se cumplen los requisitos del GDPR y las normativas de protección de datos posteriores.

Medidas organizativas	
S-O-17	Designación de una persona responsable de la protección de datos, por ejemplo, un responsable de la protección de datos
S-O-18	Protección de la totalidad de la información personal identificable en el ámbito de un sistema de gestión de la protección de datos (SGD)

5.7 Acceso remoto

Riesgo abordado Las sesiones de acceso remoto podrían ser utilizadas por personas no autorizadas como puerta de entrada a la red de BASF. Los protocolos, configuraciones, contraseñas y aplicaciones inseguros podrían permitir el acceso no autorizado.

Objetivo Durante cualquier acceso remoto, se garantiza la protección de la información y los datos almacenados, procesados y transmitidos, así como la integridad de la infraestructura de BASF.

Medidas técnicas	
S-T-17	Uso de protocolos seguros, métodos de encriptación y aplicaciones para acceder a los datos e infraestructuras de BASF.

Medidas organizativas	
S-O-19	Documentación completa o grabación de todas las sesiones de acceso remoto

5.8 Administración de TI

Riesgo abordado Una administración informática inadecuada podría provocar una interrupción o poner en peligro la infraestructura de BASF.

Objetivo Todas las actividades de servicio y asistencia se realizan de conformidad con las mejores prácticas del sector para una administración segura.

Medidas técnicas	
S-T-18	Sistema de tickets para la gestión de solicitudes de servicio y asistencia

Medidas organizativas	
S-O-20	Gestión y documentación de las herramientas utilizadas por el personal de servicio y asistencia
S-O-21	Instalación inmediata de actualizaciones y parches relevantes para la seguridad de todas las soluciones de software utilizadas.
S-O-22	Proceso de realización de las actividades de servicio y apoyo que se prestan.

6 Componentes de hardware

Adquisición de componentes de hardware individuales que se instalan en los terminales o para cuyo uso se requiere un terminal, por ejemplo, ratón, teclado, pantalla, RAM, discos duros, etc.

6.1 Entrega

Riesgo abordado Los componentes de hardware podrían dañarse durante el proceso de entrega. Además, los componentes podrían manipularse para poner en peligro la infraestructura de BASF.

Objetivo Todos los componentes de hardware se entregan completamente funcionales y en la configuración prevista en un estado íntegro.

Medidas técnicas	
H-T-01	Plataforma de recepción, tramitación y resolución de reclamaciones y devoluciones
H-O-01	Proceso para garantizar la integridad de cada entrega antes del envío
Medidas organizativas	
H-O-02	Seguimiento de envíos en tiempo real
H-O-03	Protección de los envíos frente a daños
H-O-04	Precintado de todos los envíos

6.2 Seguridad de los productos

Riesgo abordado Los componentes inadecuados, dañados o manipulados podrían provocar interrupciones o poner en peligro la infraestructura de BASF.

Objetivo Todos los componentes de hardware son probados en términos de funcionalidad e integridad por el proveedor o un proveedor anterior. Se dispone de documentación técnica suficiente sobre todos los componentes de hardware para seleccionar los componentes óptimos para una aplicación determinada.

Medidas organizativas	
H-O-05	Documentación del entorno operativo ideal para todos los componentes
H-O-06	Proceso de validación de la funcionalidad e integridad de todos los componentes por parte del proveedor o de un proveedor anterior.

7 Endpoint y dispositivos

Adquisición de dispositivos previstos para su uso por los usuarios finales o en el centro de datos, por ejemplo, ordenadores portátiles, teléfonos inteligentes, servidores, etc., así como aparatos (dispositivos de un solo uso / dispositivos con sistemas operativos especializados que son esenciales para el funcionamiento), como cortafuegos, pasarelas VPN, routers o conmutadores.

7.1 Entrega

Riesgo abordado Los dispositivos podrían resultar dañados durante el proceso de entrega. Además, los componentes podrían manipularse para poner en peligro la infraestructura de BASF.

Objetivo Todas las pruebas se entregan totalmente funcionales y con la configuración prevista en un estado íntegro.

Medidas técnicas	
E-T-01	Plataforma de recepción, tramitación y resolución de reclamaciones y devoluciones

Medidas organizativas	
E-O-01	Proceso para garantizar la integridad de cada entrega antes del envío
E-O-02	Seguimiento de envíos en tiempo real
E-O-03	Protección de los envíos frente a daños
E-O-04	Precintado de todos los envíos

7.2 Seguridad de los productos

Riesgo abordado Los dispositivos inadecuados, dañados o manipulados podrían provocar interrupciones o poner en peligro la infraestructura de BASF.

Objetivo Todos los dispositivos son probados en términos de funcionalidad e integridad por el proveedor o un proveedor anterior. Se dispone de documentación técnica suficiente sobre todos los componentes de hardware para seleccionar los componentes óptimos para una aplicación determinada.

Medidas organizativas	
E-O-05	Documentación del entorno operativo ideal para todos los componentes
E-O-06	Proceso de validación de la funcionalidad e integridad de todos los componentes por parte del proveedor o de un proveedor anterior.

7.3 Configuración del dispositivo

Riesgo abordado Cuando los dispositivos son configurados inicialmente por el proveedor, el uso de configuraciones por defecto comunes y, por tanto, fáciles de adivinar, podría permitir a los atacantes poner en peligro BASF.

Goal Las actualizaciones y parches relacionados con la seguridad disponibles en el momento de la instalación se instalan en todos los dispositivos. Las contraseñas iniciales están configuradas de forma que deben ser cambiadas por el usuario en el primer inicio de sesión.

Medidas organizativas	
E-O-07	Instalación de todas las actualizaciones y parches disponibles para el sistema operativo y el firmware.
E-O-08	Uso de contraseñas iniciales, que deben cambiarse cuando se utiliza el dispositivo por primera vez.
E-O-09	Evitar la instalación de paquetes de software que no sean esenciales, por ejemplo, software OEM opcional.

8 Soluciones in situ

Adquisición de aplicaciones (paquetes) que se ejecutan en la infraestructura de BASF (por ejemplo, en ordenadores portátiles, servidores o teléfonos inteligentes) y no requieren acceso a los sistemas del fabricante para su uso.

8.1 Concepto de seguridad informática

Riesgo abordado Si no se tienen en cuenta los mecanismos de seguridad estándar de la industria durante la planificación y el desarrollo, o si no se reconocen las interacciones entre las medidas, los atacantes podrían explotar las vulnerabilidades de seguridad resultantes y comprometer la información, los datos y la infraestructura de BASF.

Objetivo La totalidad de todas las medidas de seguridad de una solución se definen en el ámbito de un concepto de seguridad informática, y el estado de aplicación se documenta y actualiza continuamente cuando se realizan cambios.

Medidas organizativas	
O-O-01	Desarrollo de un concepto de seguridad informática para la solución
O-O-02	Actualización periódica del concepto de seguridad informática y en caso de cambios
O-O-03	Suministro a BASF de documentación sobre los mecanismos de seguridad aplicados

8.2 Criptografía

Riesgo abordado Si los datos no están protegidos durante su almacenamiento, tratamiento o transmisión, podrían ser interceptados o comprometidos por terceros no autorizados.

Objetivo Durante todo el ciclo de vida, los datos están protegidos de accesos no autorizados.

Medidas técnicas	
O-T-01	Cifrado de datos durante la transferencia (Datos en tránsito), por ejemplo HTTPS, SSH
O-T-02	Cifrado de datos durante el almacenamiento, por ejemplo, cifrado de bases de datos

O-T-03	Autenticación multifactor para acceder a información sensible
O-T-04	Autenticación multifactor para cambios de configuración

Medidas organizativas

O-O-04	Concepto criptográfico con todos los métodos de cifrado y longitudes de clave implementados.

8.3 Concepto de funciones y permisos

Riesgo abordado Un concepto de funciones y permisos inexistente o inadecuado podría permitir a usuarios no autorizados acceder a información sensible.

Objetivo Los roles y permisos pueden gestionarse de forma granular para que los usuarios sólo tengan acceso a la información que necesitan para realizar sus tareas.

Medidas técnicas

O-T-05	API de Active Directory
O-T-06	API LDAP
O-T-07	Asignación de permisos exclusivamente mediante la asignación de funciones
O-T-08	Módulo de software / componente / función para la gestión de roles y permisos

Medidas organizativas

O-O-05	Concepto formalizado y documentado de funciones y permisos

8.4 Actualizaciones y parches

Riesgo abordado Si las actualizaciones y los parches relevantes para la seguridad no se instalan inmediatamente después de su publicación, los atacantes podrían reconstruir la vulnerabilidad abordada por la actualización o el parche y explotarla activamente.

Objetivo El tiempo que transcurre entre la publicación de las actualizaciones y los parches, su suministro a BASF y su instalación es tan corto que hace imposible que los atacantes exploten activamente las vulnerabilidades conocidas que no han sido corregidas.

Medidas técnicas	
O-T-09	Suministro de actualizaciones y parches relacionados con la seguridad dentro de la solución
O-T-10	Suministro de actualizaciones y parches relacionados con la seguridad a través del sitio web del proveedor.

Medidas organizativas	
O-O-06	Información por correo electrónico sobre nuevas actualizaciones y parches
O-O-07	Información sobre nuevas actualizaciones y parches de la solución
O-O-08	Información sobre nuevas actualizaciones y parches a través del sitio web del proveedor

8.5 Pruebas de penetración

Riesgo abordado La complejidad de las soluciones puede hacer que las vulnerabilidades pasen desapercibidas debido a la interacción de los subcomponentes y los efectos resultantes. Estos puntos ciegos podrían ser aprovechados por los atacantes.

Objetivo El nivel de protección de la solución global se revisa periódicamente, teniendo en cuenta todos los métodos de ataque conocidos, y se sigue desarrollando en función de los resultados.

Medidas organizativas	
O-O-09	Pruebas periódicas de penetración de la solución
O-O-10	Pruebas de penetración de la solución basadas en eventos, por ejemplo, en caso de cambios significativos.
O-O-11	Pruebas periódicas de penetración de componentes de terceros, por ejemplo, módulos de software de desarrolladores externos.
O-O-12	Pruebas de penetración de componentes de terceros basadas en eventos, por ejemplo, cuando se identifican vulnerabilidades o incidentes de seguridad.

8.6 Asistencia y documentación para los usuarios

Riesgo abordado La ausencia o no disponibilidad de instrucciones de uso podría dar lugar a que los usuarios no utilizaran la solución o lo hicieran de forma incorrecta. Esto podría tener un efecto adverso en las operaciones de BASF.

Objetivo Todos los grupos de usuarios están habilitados para utilizar la solución de la manera prevista para el propósito previsto.

Medidas técnicas	
O-T-11	Foro comunitario para el intercambio entre usuarios
O-T-12	Sitio web de ayuda a los usuarios
O-T-13	Línea telefónica de atención a los usuarios
O-T-14	Asistencia por correo electrónico para los usuarios
Medidas organizativas	
O-O-13	Formación ofrecida a los usuarios (grupos) por los propios formadores del proveedor
O-O-14	Formación ofrecida a los usuarios (grupos) por proveedores de formación externos, por ejemplo, asociaciones industriales, TÜV (Asociación Alemana de Inspección Técnica).
O-O-15	Materiales de autoaprendizaje para usuarios (grupos), por ejemplo, vídeos tutoriales, presentaciones, instrucciones paso a paso
O-O-16	Manuales de uso general
O-O-17	Manuales de usuario basados en escenarios

8.7 Asistencia y documentación para administradores

Riesgo abordado Una instalación, distribución o configuración inadecuadas podrían poner en peligro los datos o provocar un fallo de la solución, lo que interrumpiría las operaciones de BASF.

Los administradores de **Goal** BASF responsables del funcionamiento de la solución están habilitados para gestionar la solución según lo previsto.

Medidas técnicas

O-T-15	Foro comunitario de intercambio entre administradores
O-T-16	Sitio web del servicio de asistencia para administradores
O-T-17	Línea telefónica directa para administradores
O-T-18	Asistencia por correo electrónico para administradores

Medidas organizativas

O-O-18	Formación ofrecida a los administradores por los propios formadores del proveedor
O-O-19	Formación para administradores ofrecida por proveedores de formación externos, por ejemplo, asociaciones industriales, TÜV (Organismo de Inspección Técnica).
O-O-20	Materiales de autoaprendizaje para administradores, por ejemplo, vídeos tutoriales, presentaciones, instrucciones paso a paso
O-O-21	Manuales del administrador general
O-O-22	Manuales del administrador basados en escenarios

8.8 Arquitectura de software

Riesgo abordado Si se permite el acceso desde fuera de la infraestructura de BASF a través de Internet, los atacantes podrían explotar vulnerabilidades funcionales y arquitectónicas para recuperar datos o, en caso de ataques exitosos, obtener acceso a otros sistemas dentro de la infraestructura de BASF a través de la escalada de privilegios.

Objetivo Tanto la arquitectura como los procesos para el procesamiento de datos están diseñados para proteger la solución y los datos procesados de accesos no autorizados y para garantizar que ningún otro sistema de BASF se vea afectado si los componentes individuales se ven comprometidos.

Medidas técnicas	
O-T-19	Arquitectura de 3 niveles: separación de las capas de presentación, procesamiento y almacenamiento de datos.
O-T-20	Arquitectura de 2 niveles: separación de las capas de aplicación y almacenamiento de datos
O-T-21	Protección contra secuencias de comandos en sitios cruzados
O-T-22	Validación de entradas para proteger contra la manipulación no autorizada de datos, por ejemplo, mediante inyección SQL.
Medidas organizativas	
O-O-23	Documentación de la arquitectura de la solución

9 Soluciones en la nube

Adquisición de aplicaciones (paquetes) que funcionan en la infraestructura de un proveedor de servicios y cuyo uso requiere acceso obligatorio a internet. Es irrelevante si una solución es SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), Iaas (Infrastructure-as-a-Service) o una tecnología en nube que no es específica aquí.

9.1 Concepto de seguridad informática

Riesgo abordado Si no se tienen en cuenta los mecanismos de seguridad estándar de la industria durante la planificación y el desarrollo, o si no se identifican las interacciones entre las medidas, los atacantes podrían explotar las vulnerabilidades resultantes y comprometer la información, los datos y la infraestructura de BASF.

Objetivo La totalidad de todas las medidas de seguridad de una solución se definen en el ámbito de un concepto de seguridad informática, y el estado de aplicación se documenta y actualiza continuamente cuando se realizan cambios.

Medidas organizativas	
CL-O-01	Desarrollo de un concepto de seguridad informática para la solución
CL-O-02	Actualización periódica del concepto de seguridad informática y en caso de cambios
CL-O-03	Suministro a BASF de documentación sobre los mecanismos de seguridad aplicados

9.2 Criptografía

Riesgo abordado Si los datos no están protegidos durante su almacenamiento, tratamiento o transmisión, podrían ser interceptados o comprometidos por terceros no autorizados.

Objetivo Durante todo el ciclo de vida, los datos están protegidos de accesos no autorizados.

Medidas técnicas	
CL-T-01	Cifrado de datos durante la transferencia (Datos en tránsito), por ejemplo HTTPS, SSH
CL-T-02	Cifrado de datos durante el almacenamiento, por ejemplo, cifrado de bases de datos
CL-T-03	Autenticación multifactor para acceder a información sensible
CL-T-04	Autenticación multifactor para cambios de configuración
Medidas organizativas	
CL-O-04	Concepto criptográfico con todos los métodos de cifrado y longitudes de clave implementados.

9.3 Concepto de funciones y permisos

Riesgo abordado Un concepto de funciones y permisos inexistente o inadecuado podría permitir a usuarios no autorizados acceder a información sensible.

Objetivo Los roles y permisos pueden gestionarse de forma granular para que los usuarios sólo tengan acceso a la información que necesitan para realizar sus tareas.

Medidas técnicas	
CL-T-05	API de Active Directory
CL-T-06	API LDAP
CL-T-07	Asignación de permisos exclusivamente mediante la asignación de funciones
CL-T-08	Módulo de software / componente / función para la gestión de roles y permisos

Medidas organizativas	
CL-O-05	Concepto formalizado y documentado de funciones y permisos

9.4 Protección contra malware

Riesgo abordado Si los sistemas se ven comprometidos, la información podría modificarse involuntariamente o ponerse al alcance de terceros no autorizados.

Objetivo Se garantiza que no puedan instalarse programas maliciosos en los dispositivos informáticos.

Medidas técnicas	
CL-T-09	Solución de protección contra malware para servidores Windows
CL-T-10	Solución de protección contra malware en clientes, por ejemplo, Microsoft Defender
CL-T-11	Dispositivos de seguridad, por ejemplo, cortafuegos, SIEM
CL-T-12	Segmentación adecuada de la red corporativa basada en la criticidad con respecto a los requisitos de confidencialidad y disponibilidad de los datos procesados.
CL-T-13	Uso de una solución sandbox para abrir archivos desconocidos o de remitentes desconocidos.
CL-T-14	Distribución de software gestionada centralmente
CL-T-15	No concesión de derechos de administración local a los promotores
CL-T-16	No se conceden derechos de administración local a los usuarios

Medidas organizativas	
CL-O-06	Proceso para la instalación inmediata de actualizaciones relevantes para la seguridad de todas las soluciones de software en uso.

CL-O-07	Política de refuerzo de servidores
CL-O-08	Política de endurecimiento para clientes
CL-O-09	Política de endurecimiento para smartphones

9.5 Copia de seguridad de datos

Riesgo abordado Los errores del sistema, los programas maliciosos o el uso indebido de los sistemas informáticos podrían provocar la pérdida de datos.

Objetivo Se realizan copias de seguridad periódicas de todos los datos relevantes para BASF, que pueden restaurarse en caso de pérdida de datos.

Medidas técnicas	
CL-T-17	Copias de seguridad periódicas y automatizadas de todos los datos relevantes para BASF.
CL-T-18	Flujo de trabajo de despliegue automatizado, por ejemplo CI/CD

Medidas organizativas	
CL-O-10	Concepto de copia de seguridad
CL-O-11	Ejercicios regulares de copia de seguridad y recuperación de datos
CL-O-12	Instantáneas manuales de los estados del sistema antes de realizar cambios significativos en los sistemas y aplicaciones necesarios para ejecutar la solución.

9.6 Pruebas de penetración

Riesgo abordado La complejidad de las soluciones puede dar lugar a que las vulnerabilidades pasen desapercibidas debido a la interacción de los subcomponentes y los efectos resultantes. Estos puntos ciegos podrían ser aprovechados por los atacantes.

Objetivo El nivel de protección de la solución global se revisa periódicamente, teniendo en cuenta todos los métodos de ataque conocidos, y se sigue desarrollando en función de los resultados.

Medidas organizativas	
CL-O-13	Pruebas periódicas de penetración de la solución
CL-O-14	Pruebas de penetración de la solución basadas en eventos, por ejemplo, en caso de cambios significativos.
CL-O-15	Pruebas periódicas de penetración de componentes de terceros, por ejemplo, módulos de software de desarrolladores externos.
CL-O-16	Pruebas de penetración de componentes de terceros basadas en eventos, por ejemplo, cuando se identifican vulnerabilidades o incidentes de seguridad.

9.7 Asistencia y documentación para los usuarios

Riesgo abordado La falta de instrucciones de uso o la no disponibilidad de las mismas podría dar lugar a que los usuarios no utilizaran la solución o lo hicieran de forma incorrecta. Esto podría tener un efecto adverso en las operaciones de BASF.

Objetivo Todos los grupos de usuarios están habilitados para utilizar la solución de la manera prevista para el propósito previsto.

Medidas técnicas	
CL-T-19	Foro comunitario para el intercambio entre usuarios
CL-T-20	Sitio web de ayuda a los usuarios
CL-T-21	Línea telefónica de atención a los usuarios
CL-T-22	Asistencia por correo electrónico para los usuarios

Medidas organizativas	
CL-O-17	Formación ofrecida a los usuarios (grupos) por los propios formadores del proveedor
CL-O-18	Formación ofrecida a los usuarios (grupos) por proveedores de formación externos, por ejemplo, asociaciones industriales, TÜV (Asociación Alemana de Inspección Técnica).
CL-O-19	Materiales de autoaprendizaje para usuarios (grupos), por ejemplo, vídeos tutoriales, presentaciones, instrucciones paso a paso
CL-O-20	Manuales de uso general
CL-O-21	Manuales de usuario basados en escenarios

9.8 Asistencia y documentación para administradores

Riesgo abordado Una instalación, distribución o configuración inadecuadas podrían poner en peligro los datos o provocar un fallo de la solución, lo que interrumpiría las operaciones de BASF.

Los administradores de **Goal** BASF responsables del funcionamiento de la solución están habilitados para gestionar la solución según lo previsto.

Medidas técnicas	
CL-T-23	Foro comunitario de intercambio entre administradores
CL-T-24	Sitio web del servicio de asistencia para administradores
CL-T-25	Línea telefónica directa para administradores
CL-T-26	Asistencia por correo electrónico para administradores

Medidas organizativas	
CL-O-22	Formación ofrecida a los administradores por los propios formadores del proveedor

CL-O-23	Formación para administradores ofrecida por proveedores de formación externos, por ejemplo, asociaciones industriales, TÜV (Agencia de Inspección Técnica).
CL-O-24	Materiales de autoaprendizaje para administradores, por ejemplo, vídeos tutoriales, presentaciones, instrucciones paso a paso
CL-O-25	Manuales del administrador general
CL-O-26	Manuales del administrador basados en escenarios

9.9 Arquitectura de software

Riesgo abordado Los atacantes podrían explotar vulnerabilidades en la arquitectura del software para recuperar datos o, en caso de ataques exitosos, obtener acceso a otros sistemas dentro de la infraestructura de BASF a través de la escalada de privilegios.

Objetivo La arquitectura del software está diseñada para proteger la solución y los datos procesados de accesos no autorizados y para garantizar que ningún otro sistema de BASF se vea afectado si los componentes individuales se ven comprometidos.

Medidas técnicas

CL-T-27	Arquitectura de 3 niveles: separación de las capas de presentación, procesamiento y almacenamiento de datos.
CL-T-28	Arquitectura de 2 niveles: separación de las capas de aplicación y almacenamiento de datos
CL-T-29	Protección contra secuencias de comandos en sitios cruzados
CL-T-30	Validación de entradas para proteger contra la manipulación no autorizada de datos, por ejemplo, mediante inyección SQL.

Medidas organizativas

CL-O-27	Documentación de la arquitectura de la solución

9.10 Gestión de la continuidad de las actividades

Riesgo abordado El fallo o mal funcionamiento de componentes críticos del sistema puede provocar pérdidas en la disponibilidad de las soluciones en la nube. Especialmente en el caso de procesos empresariales críticos, incluso una breve interrupción puede provocar daños considerables para BASF.

Objetivo El cumplimiento de los acuerdos de nivel de servicio (SLA) acordados puede garantizarse durante toda la duración del contrato.

Medidas técnicas	
CL-T-31	Centro de datos de emergencia

Medidas organizativas	
CL-O-28	Designación de una persona responsable de la gestión de emergencias, por ejemplo, responsable de BCM, responsable de emergencias
CL-O-29	Gestión de la totalidad de las medidas de gestión de emergencias en el ámbito de un Sistema de Gestión de la Continuidad de las Actividades (SGCN)
CL-O-30	Concepto de redundancia

9.11 Protección de datos personales

Riesgo abordado Cuando se procesan datos de identificación personal en el ámbito del tratamiento contratado, los derechos personales de los interesados podrían verse comprometidos por un uso inadecuado de la información.

Objetivo Al procesar la IIP, se garantiza en todo momento que se cumplen los requisitos del GDPR y las normativas de protección de datos posteriores.

Medidas organizativas	
CL-O-31	Designación de una persona responsable de la protección de datos, por ejemplo, un responsable de la protección de datos
CL-O-32	Protección de la totalidad de la información personal identificable en el ámbito de un sistema de gestión de la protección de datos (SGD)

9.12 Seguridad física

Riesgo abordado Si las soluciones en nube funcionan en centros de datos no seguros, los servidores y otros componentes informáticos pueden ser manipulados, robados o destruidos.

Objetivo Toda la infraestructura necesaria para ofrecer la solución en la nube funciona en un centro de datos seguro.

Medidas técnicas	
CL-T-32	Sistema de extinción y prevención de incendios
CL-T-33	Compartimentos de incendios múltiples
CL-T-34	Sistema de alarma
CL-T-35	Sistema de videovigilancia
CL-T-36	Supervisión automatizada de la infraestructura
CL-T-37	Conexión del centro de datos a un puesto de control central, atendido las 24 horas del día, los 7 días de la semana.
CL-T-38	Gestión de la temperatura y la humedad
CL-T-39	Sistema de alimentación ininterrumpida
CL-T-40	Dispositivo de protección contra sobretensiones
Medidas organizativas	
CL-O-33	Medidas de protección contra el polvo
CL-O-34	Concepto de control de acceso

10 Desarrollo de software

Desarrollo de soluciones o componentes de software que se utilizan de forma independiente o en integración con otras soluciones. También incluye la personalización de soluciones. La configuración de una solución no entra dentro del desarrollo de software.

Nota sobre la aplicación: Los requisitos para el desarrollo de software deben cumplirse además de los tipos de servicio Soluciones locales y Soluciones en la nube cuando los proveedores desarrollen soluciones por sí mismos.

10.1 Proceso de desarrollo

Riesgo abordado Si no se aplican las mejores prácticas para el desarrollo seguro de software, esto puede dar lugar a vulnerabilidades de seguridad que podrían ser explotadas por atacantes. Esto se aplica tanto al código fuente como a la configuración de los medios de instalación suministrados.

Objetivo Un proceso de desarrollo estandarizado y gestionado garantiza que se cierran todas las vulnerabilidades conocidas del software (paquetes) en uso y que los medios de instalación se configuran de forma suficientemente segura antes de su despliegue.

Medidas técnicas	
SW-T-01	Flujo de trabajo de despliegue automatizado, por ejemplo CI/CD

Medidas organizativas	
SW-O-01	Ciclo de vida formalizado para el desarrollo seguro de software (SSDLC)
SW-O-02	Gestión y documentación de las herramientas utilizadas en el proceso de desarrollo
SW-O-03	Pruebas de nuevas versiones de la solución basadas en casos de prueba normalizados
SW-O-04	Realización de pruebas unitarias
SW-O-05	Realización de pruebas de carga
SW-O-06	Adhesión al principio: seguridad por diseño
SW-O-07	Adhesión al principio: seguridad por defecto
SW-O-08	Adhesión al principio Privacidad desde el diseño
SW-O-09	Adhesión al principio Privacidad por defecto

10.2 Software de terceros

Riesgo abordado Cuando se utilizan componentes de software de terceros, como módulos de software de desarrolladores externos, las vulnerabilidades en estos componentes podrían servir como vectores de ataque para que los atacantes obtengan acceso no autorizado a los datos.

Objetivo Todos los componentes de software de terceros se comprueban periódicamente para detectar vulnerabilidades. Las actualizaciones y parches relevantes para la seguridad de los componentes externos son proporcionados por el proveedor a través del canal general de actualizaciones y parches acordado para la solución.

Medidas organizativas	
SW-O-10	Registro de todos los componentes de software de terceros
SW-O-11	Proceso de comprobación periódica de las vulnerabilidades conocidas de los componentes de software de terceros utilizados.