Política de Seguridad de la Información, Calidad y Continuidad

EAD Trust — European Agency of Digital Trust

Código documento		**Nombre descriptivo**		**Difusión**
NOR-PG-Seguridad-Informacion-Calidad-Continudad		Política de Seguridad de la Información, Calidad y Continuidad		Pública
Código de área		**Tipo documental**		**Revisión periódica**
NOR		Política		Anual
Versión	**Fecha**	**Responsable**	**Descripción**	
4	06/07/2026	Compliance	Versión original	
Fecha revisión	**Versión revisada**	**Revisado por**	**Descripción revisión**	
3	25-10-2025	Resp. Compliance	Se incorpora la política de continuidad.	
2	13-10-2025	Resp. Compliance	Se incorpora la política de calidad.	
1	01-05-2025	Resp. Compliance	Primera versión.	
Aprobado por				

Firmado por ***9451** EDUARDO INZA (EAD ****2624*) el día 06/07/2026 con un certificado emitido por EADTrust RSA 4096

Índice

1. Introducción y objeto

La Dirección de EAD Trust es consciente de la importancia de la calidad y la seguridad de la información a la hora de satisfacer las necesidades de sus clientes y otras partes interesadas, proporcionando productos y servicios de alta calidad, así como es su obligación garantizar el cumplimiento de los requisitos legales y otras normativas aplicables a sus actividades como Prestador Cualificado de Servicios de Confianza, así como el resto de las actividades que realiza.

Como proveedor de servicios de confianza, cualquier brecha en la seguridad de la información (incluida la pérdida o el robo) puede provocar la inmediata pérdida de confianza de todos los stakeholders del mercado y, por tanto, la inviabilidad de nuestra agencia. Es decir, la seguridad de la información es la máxima prioridad de EAD Trust.

Se ha implantado un Sistema Integrado de Gestión de Calidad y de Gestión de la Seguridad de la Información para mejorar sus métricas de Calidad y Seguridad, de cara a proveedores, a clientes, y a organismos de Evaluación de Conformidad y de Supervisión. La política de seguridad de la información acompaña a la Política de Calidad y a la de Gestión de Servicios, además de estar supeditada a la Política de Gestión del Cambio.

Debido a la importancia de la seguridad de la información en la operativa de la empresa y a la dificultad de asimilar distintos documentos de políticas, en el 2020 se decidió unificar la mayoría de las políticas temáticas bajo este documento. Las políticas de Recursos Humanos, Protección de datos personales, uso de controles criptográficos, accesos y seguridad física, se mantienen separadas debido a su complejidad e importancia en operativas críticas.

Se promueve la mejora continua de los servicios, procesos y actividades, como objetivo permanente de EAD Trust, así como sostener e incrementar la seguridad de la información y la satisfacción del cliente.

2. Alcance

Esta política es de aplicación a:

- Todas las áreas y procesos de la organización.
- Todo el personal, que tendrá que garantizar que todos los procedimientos, servicios y activos de la empresa con capacidad para almacenar o procesar datos cumplen estas políticas.
- Los recursos, sistemas e información necesarios para la actividad.
- Los proveedores y terceros críticos, cuando proceda.

3. Marco normativo y de cumplimiento

EAD Trust se rige por la legislación europea y española y diferentes estándares técnicos internacionales aplicables a los Prestadores de Servicios Electrónicos de Confianza, así como la normativa europea y española de Protección de datos y Seguridad. En particular:

- Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo).
- Normas ISO 27001 (Sistema de gestión de la seguridad de la información).
- ISO 9001 (sistema de gestión de calidad).
- ISO 20000-1 (gestión de servicios de TI).
- Estándares ETSI (ETSI-EN-319-401, ETSI-EN-319-411-1, ETSI-EN-319-421...).
- Reglamento eIDAS (UE 910/2014) y eIDAS 2.
- Normativa de Protección de Datos: Reglamento (UE) 2016/679 (RGPD) y Ley Orgánica 3/2018 (LOPDGDD).

También es de aplicación la regulación general que pueda afectar a su actividad. La organización posee un registro por el cual se controla y se mantiene actualizado el conjunto de la normativa, bajo el nombre NOR-RG-Normativa_EADTrust.

Las auditorías de certificación ISO 9001, ISO 27001 e ISO 20000-1, así como ENS de nivel alto y auditorías eIDAS reflejan el compromiso de la entidad respecto a la adopción de una cultura de mejora continua en todas las actividades y la percepción de las mejoras por los clientes y demás partes interesadas, que redunde en un aumento de su satisfacción.

Esta política proporciona referencia, orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes y, en particular, con relación al Esquema Nacional de Seguridad.

4. Definición de la seguridad de la información

EAD Trust define la seguridad de la información como el conjunto de sistemas tecnológicos y de medidas preventivas y reactivas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

El sistema de gestión documental adoptado para la aprobación de otras políticas y procedimientos que describen las tareas cuya ejecución se requieren para la adopción de las referidas medidas, se establece en la guía para la gestión de la documentación EAD Trust NOR-PRD-Control-documental.

5. Objetivos de seguridad de la información

EAD Trust considera que una gestión adecuada de la calidad y de la seguridad de la información es fundamental, por un lado, para que sus servicios sean atractivos para sus clientes y, por otro, para asegurar la continuidad del servicio, minimizando daños potenciales de origen informático. Entre los objetivos de seguridad de la información que se contemplan están:

Confidencialidad: La información confidencial de la empresa debe ser conocida únicamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.

Integridad: La información de la empresa debe ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación, sin que se vea afectada por causas externas o incidentes internos.

Disponibilidad: La información de la empresa debe ser accesible y utilizable por los usuarios autorizados quedando garantizada su propia persistencia ante cualquier circunstancia prevista.

Autenticación: El acceso a la información de la empresa debe estar limitado a los usuarios o entidades autorizadas, identificados de manera unívoca.

Trazabilidad: El acceso a la información de la empresa debe quedar registrado, identificado su origen y las diferentes etapas de un proceso.

6. Principios de actuación

6.1. Principio de confianza

Los pilares de la confianza son la hipótesis de una conducta futura y su cumplimiento. Por lo tanto, EAD Trust, su personal y cada uno de los servicios, sistemas, activos y procedimientos

actuará de manera que la expectativa del servicio prestado y el resultado sean lo mismo o al menos lo más parecidos posible.

Este principio debe estar presente, con mayor atención, en la documentación del sistema integrado de gestión de la información y en las contrataciones con clientes y proveedores.

6.2. Principio de clasificación

Toda la información utilizada en la empresa podrá tener asignada una clasificación de seguridad. En caso de que no tenga una clasificación explícitamente designada, deberá considerarse que la clasificación es "Uso Interno". La información se protegerá de acuerdo a los riesgos asociados a su clasificación de seguridad.

6.3. Principio de separación de roles

Existe separación de roles cuando es necesaria e insoslayable la presencia de dos o más personas para llevar a cabo una operativa acogida a este principio.

Todos los servicios críticos se servirán del principio de separación de roles (también llamado de 4 ojos) para maximizar la seguridad de las actividades de gestión de servicios de confianza.

6.4. Principio de mínimo acceso

Solamente se otorgarán los mínimos permisos de seguridad necesarios para cumplir las responsabilidades de cada rol y poder realizar las tareas encomendadas. Los privilegios se mantendrán durante el menor tiempo posible una vez no sean necesarios.

6.5. Principio de cumplimiento

EAD Trust y su personal velarán por el cumplimiento de los reglamentos, normas, estándares y leyes vigentes, integrando estos requisitos con las políticas, procedimientos y sistemas correspondientes, y practicándolos en su trabajo.

6.6. Principio de necesidad de conocer

Los usuarios recibirán acceso a aquellos sistemas necesarios para poder llevar a cabo sus funciones y responsabilidades.

7. Aspiraciones y compromisos de calidad

Con la presente política se pretende cumplir un conjunto de aspiraciones:

- Llegar a ser la empresa líder en el sector de la Confianza Digital y que el cliente lo perciba por la gestión de la relación, con un alto nivel de profesionalidad y un alto grado de satisfacción de sus expectativas. En la excelencia se busca la integración de requisitos tecnológicos y legales complejos a nivel nacional y supranacional.

- Estar pendientes de las necesidades de nuestros clientes, recibiendo sus consultas y sugerencias, atendiendo de forma destacada a la identificación de nuevas necesidades y la mejora de la calidad de nuestros servicios.
- Mejorar continuamente nuestros procesos e incorporar otros nuevos conforme lo exigen nuevos requisitos legales, como eIDAS o eIDAS 2. En ese esfuerzo se considerará el marco establecido por el Sistema de Gestión de la Calidad y de la Seguridad de la Información.
- Favorecer un entorno laboral estimulante y agradable que promueva la cooperación, con la expectativa de incentivar la motivación de los empleados y su compromiso con la mejora continua y la satisfacción de nuestros clientes.
- Satisfacer las necesidades formativas de los empleados y facilitar documentación técnica y jurídica a otras partes interesadas.
- Desplegar sistemas que den soporte a la continuidad del negocio desarrollando e implantando planes de continuidad de conformidad con las normas sectoriales.
- Realizar una evaluación continua de riesgos en las actividades que desarrollamos y el consecuente despliegue de medidas de remediación en el contexto de nuestra cultura de gestión de calidad y de seguridad.

Para la consecución de estos objetivos es fundamental la colaboración del personal de la entidad, que contará con el apoyo de la Dirección.

8. Organización, roles y responsabilidades

La Dirección declara su compromiso con el Sistema de Gestión Integrado promoviendo y comunicando las políticas de la entidad en las diferentes áreas, incluso de forma abierta en su página web.

En los procedimientos internos de la entidad se establecen roles y responsabilidades del personal. Todo el personal de EAD Trust contribuye a alcanzar y mantener un nivel de desempeño en los procesos de la entidad acorde a los requisitos de los clientes y demás partes interesadas.

8.1. Estructura de gobierno

Se ha nombrado un Comité con los perfiles profesionales necesarios para garantizar las funciones de Comité de Seguridad de la Información de los Sistemas y de Organización y Planificación de EAD Trust. El Comité está formado por los siguientes miembros fijos que se reúnen con una periodicidad aproximada de quince días:

- Dirección.
- Tech Policy Officer.
- Chief Trust Officer.
- Responsable de Infraestructura y operaciones.
- Responsable de Cumplimiento.

- Responsable de Proyectos.

El Comité asume su responsabilidad y nombramiento con la formalización de los nombramientos en un acta. El resto de perfiles de EAD Trust pueden participar de forma activa en el Comité en momentos en los que sea necesario.

9. Objetivos de control de seguridad

9.1. Información e información de autenticación

La información deberá:

- Clasificarse de acuerdo a los niveles de secreto.
- Protegerse en función de su clasificación de seguridad.
- Ser protegida en las redes y recursos de tratamiento de la información.
- Evitarse su pérdida mediante copias de seguridad.
- Gestionarse con especial cuidado cuando se encuentre en soportes extraíbles.
- Destruirse antes de su enajenación.

En particular, la información de autenticación tendrá la clasificación de «Reservado» y deberá:

- Ser controlada a través de un proceso formal de gestión.
- Ser salvaguardada por cada usuario, como responsable de la misma.
- Seguir las prácticas de la organización.
- Usar un sistema de gestión de contraseñas interactivo.

9.2. Seguridad de la información en procesos

La seguridad de la información deberá:

- Ser tratada dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.
- Mantenerse durante las transferencias con entidades externas.
- Garantizarse en el ciclo de vida del desarrollo de software de acuerdo a las restricciones propias de la clasificación de la seguridad procesada.
- Asegurarse con proveedores externos mediante SLA.
- Revisarse para garantizar que se implementa y opera de acuerdo a las políticas y procedimientos de la organización.
- Formar parte de la continuidad de negocio. El detalle de la gestión de continuidad se desarrolla en la sección 12 de esta política.

9.3. Activos, personal, personal de confianza y eventos de seguridad

9.3.1. Activos

Los activos deberán ser:

- Identificados y sus responsabilidades de protección deberán ser adecuadamente definidas.
- Verificados respecto a la integridad del software en explotación.
- Custodiados contra la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización, asegurando la disponibilidad de los activos críticos.
- Protegidos contra el malware.
- Resguardados contra modificaciones de software no autorizadas.
- Defendidos contra la explotación de vulnerabilidades técnicas.
- Borrados antes de destinarlos a otro uso.

9.3.2. Personal

Todo el personal deberá:

- Comportarse lealmente, contribuyendo a los objetivos definidos en las políticas de la empresa.
- Oponerse y negar su apoyo a cualquier filtración o brecha de seguridad, incluyendo cualquier información clasificada como de “Uso Interno” o más secreta.

9.3.3. Personal de confianza

El personal de confianza será:

- Designado por un proceso documentado.
- Autorizado explícitamente a acceder a zonas seguras y de alta seguridad.
- Asignado a seguir incidentes de seguridad.
- Vigilante de los principios de menor privilegio y separación de roles.

9.3.4. Eventos y vulnerabilidades de seguridad

Los eventos y vulnerabilidades de seguridad deberán ser:

- Registrados.
- Procesados y gestionados de manera coherente y eficaz, siendo analizados en menos de 48 horas.
- Escalados mediante alarma.
- Comunicados de acuerdo a los requisitos vigentes.

10. Políticas específicas de seguridad

10.1. Política de datos

10.1.1. Recogida de datos

EAD Trust siempre recogerá la menor cantidad de datos y evidencias necesarias para llevar a cabo sus servicios, manteniendo la privacidad de los datos que marquen las leyes vigentes.

10.1.2. Datos de prueba

El uso de datos reales para pruebas está sujeto a las restricciones de seguridad de la fuente original de los datos. En general, se desaconseja el uso de datos personales reales para pruebas en cualquier entorno.

No está autorizado el uso de datos reales personales, financieros o médicos en entornos de test o desarrollo y se requiere aprobación expresa de la dirección para utilizarlos en entornos de preproducción durante las pruebas finales previas a un despliegue.

Cuando se utilicen datos reales para pruebas siempre se utilizarán copias de los mismos. El tiempo de vida de estas copias será efímero y el proceso deberá garantizar su destrucción una vez terminadas las pruebas.

10.2. Política de dispositivos móviles y BYOD

No se permite el uso de dispositivos móviles personales para actividades de trabajo o teletrabajo ni el almacenamiento de datos corporativos con nivel de clasificación superior a Público en cualquier dispositivo personal, ya sea total o parcialmente.

Excepcionalmente y bajo autorización, podrá permitirse el acceso a herramientas de comunicación como el correo electrónico desde estos dispositivos.

10.3. Política de escritorio despejado y pantalla limpia

La información con clasificación de seguridad “Difusión Limitada” o más secreta deberá estar guardada cuando no se necesite, independientemente de su soporte (en papel o cualquier almacenamiento electrónico). Además, cuando se imprima este tipo de información, se deberá retirar de la impresora inmediatamente.

Los ordenadores y terminales deben quedarse apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado controlado mediante una contraseña, dispositivo hardware o mecanismo similar de autenticación de usuario cuando estén desatendidos y deben estar protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso.

10.4. Política de uso de sistemas

El uso aceptable de los sistemas corporativos de gestión de información se regula en el documento CAL-PE-Política de buen uso de los sistemas corporativos de gestión de información.

11. Política de compras y evaluación de proveedores

Esta política de compras tiene como objetivo establecer los principios que rigen durante el proceso de compras de EAD Trust y la sistemática de evaluación de los proveedores. Se realiza para garantizar la calidad y seguridad de los bienes y servicios que se adquieren; así como del cumplimiento de los requisitos normativos en los que se basa nuestro Sistema Integrado de Gestión.

Con esta política también se busca dar a conocer a nuestros proveedores la forma en que valoramos sus servicios y los criterios de valoración para elegir a esos proveedores. La política busca complementar al procedimiento de evaluación de proveedores.

11.1. Principios de compras

Los procesos de compra se realizan teniendo en cuenta los siguientes principios:

- Transparencia y objetividad en la evaluación y selección de proveedores.
- Cumplimiento normativo, asegurando que los proveedores actúan conforme a la legislación aplicable, normativa de seguridad y estándares internacionales.
- Seguridad de la información, que garantice que los productos y servicios adquiridos no comprometan la confidencialidad, la integridad y la disponibilidad de los sistemas o datos.
- Mejora continua, mediante sistemas de evaluación.
- Sostenibilidad, fomentando, dentro de lo posible, el uso eficiente de recursos y la gestión de residuos.

11.2. Criterios de evaluación de proveedores

Los proveedores están sujetos a una evaluación basada en los principios establecidos en el documento interno de EAD Trust, que son los siguientes:

- Relación calidad/precio adecuada.
- Producto/servicio acorde a necesidad.
- Cumplimiento de plazos.
- Descuentos especiales, facilidades en el pago.
- Exclusividad del producto.
- Priorización de nuestro pedido en urgencia.
- Aporta soluciones en caso de problemas.
- Controla y mide los residuos generados.
- Gestión adecuada de residuos peligrosos (si aplica).
- Dispone de un dispositivo certificado de firma.

11.3. Clasificación de proveedores

Tras la evaluación del proveedor, este se clasificará como aprobado, aprobado condicional o rechazado. Si existen incidencias graves por parte de los proveedores aprobados o aprobados condicionales, estos pasarán a rechazado.

11.4. Controles sobre suministros externos

Las compras se realizan conforme a las necesidades operativas y de prestación de servicios de EAD Trust, teniendo en cuenta que:

- Se establecen los controles adecuados sobre los productos y servicios suministrados externamente.
- Se tiene en cuenta el impacto que dichos servicios o productos puedan tener sobre los requisitos del cliente y sobre la seguridad y continuidad del negocio.

EAD Trust informa públicamente que todos los proveedores y subcontratistas pueden ser evaluados y reevaluados en cualquier momento, conforme a los criterios establecidos en esta política y en los demás procedimientos internos que forman el SIG.

La colaboración con EAD Trust implica la aceptación implícita de esta política y del compromiso con los estándares de calidad, seguridad y cumplimiento establecidos por la organización.

11.5. Requisitos de seguridad en la adquisición de nuevos componentes

Toda adquisición de un nuevo componente del sistema de información —físico o lógico— quedará sujeta a un proceso formal de planificación que garantice el cumplimiento de la medida op.pl.3 «Adquisición de nuevos componentes» del Esquema Nacional de Seguridad. Con carácter previo a la decisión de compra, la unidad promotora deberá acreditar que la adquisición:

- Atiende a las conclusiones del análisis de riesgos del sistema.
- Es acorde a la arquitectura de seguridad escogida por la organización.
- Contempla, de forma conjunta, las necesidades técnicas, de formación y de financiación asociadas al nuevo componente.

En la práctica, la determinación de la adquisición se sustentará en la recopilación y conservación de las siguientes evidencias, que se incorporarán al expediente de compra:

- Referencia o extracto del análisis de riesgos vigente que justifique la necesidad del componente y su contribución al tratamiento de los riesgos identificados.
- Análisis de encaje en la arquitectura de seguridad, que documente la compatibilidad del componente con las líneas de defensa, los mecanismos de identificación y autenticación y el resto de elementos definidos en la arquitectura.
- Valoración conjunta de necesidades técnicas, de formación y de financiación, incluyendo los requisitos funcionales de seguridad exigidos al componente y la previsión de recursos para su operación segura.

- Cuando proceda por la categoría del sistema, verificación de que el producto o servicio figura en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) del CCN o cuenta con la certificación exigida, conforme a la medida op.pl.5 «Componentes certificados».

La documentación anterior deberá quedar formalmente aprobada por el responsable competente con carácter previo a la formalización de la compra y se conservará como evidencia de cumplimiento a efectos de auditoría del ENS.

12. Política de continuidad de negocio

12.1. Objeto

La presente Política de Continuidad de Negocio tiene por objeto establecer los principios, criterios y marco general de actuación de EAD Trust para garantizar la continuidad de sus actividades esenciales ante incidentes graves, interrupciones operativas, crisis o desastres que puedan afectar a las personas, los procesos, la tecnología, las instalaciones, los proveedores o la información.

Esta Política persigue minimizar el impacto de las interrupciones, proteger a las personas y los activos de la organización, mantener la prestación de los servicios críticos y asegurar una recuperación ordenada dentro de unos plazos aceptables.

12.2. Alcance

Esta Política aplica a todas las áreas y procesos de la organización; todo el personal; los recursos, sistemas e información necesarios para la actividad; y los proveedores y terceros críticos, cuando proceda.

12.3. Compromiso de la Dirección

La Dirección se compromete a:

- Proteger la continuidad de las actividades críticas.
- Asignar los recursos necesarios.
- Definir y mantener un sistema de continuidad de negocio.
- Revisar periódicamente su eficacia.
- Impulsar la mejora continua.

12.4. Principios de actuación

EAD Trust actuará conforme a los siguientes principios:

- Proteger a las personas.
- Priorizar los procesos críticos.

- Establecer medidas de prevención, respuesta y recuperación.
- Reducir los tiempos de interrupción y sus impactos.
- Probar y revisar periódicamente los planes.
- Mejorar continuamente el sistema de continuidad.

12.5. Responsabilidades

12.5.1. Dirección

Aprueba esta Política, apoya su implantación y revisa su eficacia.

12.5.2. Responsable del SGI

Coordina el sistema, impulsa los análisis y planes, y supervisa pruebas y revisiones.

12.5.3. Responsables de área

Identifican actividades críticas, mantienen la información actualizada y aplican las medidas definidas.

12.5.4. Personal

Debe conocer las pautas que le apliquen, participar en formación y colaborar en caso de incidente.

12.6. Marco de continuidad de negocio

La organización mantendrá, de forma proporcional a su actividad y riesgos:

- Identificación de procesos y recursos críticos.
- Análisis de impacto en el negocio (BIA).
- Análisis de riesgos.
- Estrategias y planes de continuidad y recuperación.
- Estructura de gestión de incidentes o crisis.
- Pruebas, revisiones y acciones de mejora.

12.7. Activación

Los planes de continuidad se activarán cuando una interrupción afecte, o pueda afectar de forma grave, a los procesos críticos, servicios esenciales o compromisos de la organización.

La activación, gestión y cierre de la situación se realizará conforme a los procedimientos internos definidos.

12.8. Formación, pruebas y revisión

La organización promoverá la formación y concienciación necesarias en materia de continuidad de negocio.

Asimismo, revisará esta Política y los planes asociados para asegurar que siguen siendo adecuados, eficaces y actualizados.

12.9. Mejora continua

Las incidencias, resultados de pruebas, auditorías, revisiones y cambios relevantes en la organización se utilizarán para mejorar continuamente el sistema de continuidad de negocio.

13. Comunicación, aprobación, revisión y vigencia

El Sistema Integrado de Gestión de Calidad y Seguridad de la Información ha sido elaborado y se mantiene de forma que se priorice la prevención de las desviaciones frente a la remediación de las mismas de manera reactiva. La entidad posee un procedimiento de gestión documental que garantiza la eficiencia de dicho Sistema Integrado de Gestión de Calidad y Seguridad de la Información.

La empresa se compromete a mantener actualizado a todo su personal en materia de Seguridad y velar por el cumplimiento de los requisitos establecidos en la legislación vigente en materia de Seguridad de la Información. Asimismo, se invertirá en la mejora continua del sistema siguiendo las mejores prácticas vigentes.

Esta política no será obstáculo para el desarrollo de Declaraciones de Políticas de Seguridad o Políticas de Servicios Electrónicos de Confianza específicas para el cumplimiento de determinados requisitos normativos o voluntarios. En todo caso, las citadas Declaraciones de Políticas de Seguridad y de Políticas de Servicios Electrónicos de Confianza específicas serán coherentes con la presente política.

La última versión de la política estará disponible en la web de EAD Trust.

La política se revisa con carácter anual, y con carácter extraordinario cuando ocurran situaciones especiales o cambios sustanciales en el SGI, o cambios legales que se deban considerar. La Dirección es la responsable de aprobar la política de seguridad.

La política se comunica al personal de la organización en el momento de su incorporación, así como ante cuaquier cambio significativo; este tipo de cambios también serán comunicados a los clientes, proveedores que apliquen, organismos de evaluación, supervisión u otros organismos reguladores.

14. Incumplimientos y remediación

Cualquier incumplimiento de los requisitos establecidos en materia de calidad y de seguridad de la información que se detecte llevará aparejado un proceso de remediación.

15. Aprobación

La presente Política de Seguridad de la Información, Calidad y Continuidad ha sido aprobada por la Dirección de EAD Trust y es de aplicación desde su publicación en la página web.