NORMA SELLO DATATRUST - NOBLESSE			
	Fecha Revisión: 12/10/2025	**Revisó:** CTO Noblesse	**Código:** DTN-ICS-001

Estándar de Certificación en Ciberseguridad, Privacidad y Confianza Digital

1. Introducción

En el contexto de una economía digital global e interconectada, la gestión segura y ética de la información se ha erigido como un imperativo estratégico para las organizaciones. La Norma **DataTrust Noblesse (DTN)**, desarrollada por Noblesse SpA, establece un marco integral, verificable y de alto nivel para evaluar y certificar los sistemas de gestión de ciberseguridad, privacidad y confianza digital.

El propósito fundamental de esta norma es proporcionar un marco de referencia robusto que permita a las organizaciones demostrar, de manera objetiva y auditada, su adhesión a los principios de confidencialidad, integridad, disponibilidad, transparencia y resiliencia en el tratamiento de datos personales y activos de información críticos. **El Sello DataTrust Noblesse** constituye el distintivo tangible que acredita el cumplimiento de estos rigurosos requisitos, funcionando como un sello de garantía que fortalece la reputación y fomenta relaciones de confianza sostenibles con clientes, socios, reguladores y la sociedad en general.

2. Alcance y Aplicabilidad

La Norma DataTrust Noblesse es de aplicación genérica y está diseñada para ser implementada por cualquier organización, con independencia de su tamaño, sector de actividad, naturaleza jurídica o complejidad tecnológica. Su ámbito de aplicación incluye, de manera no exhaustiva, a:

- Empresas del sector privado (PYMES y grandes corporaciones).
- Instituciones del sector público y organismos gubernamentales.
- Organizaciones sin fines de lucro (ONG).
- Proveedores de servicios tecnológicos, financieros y de salud.
- Plataformas de comercio electrónico y economía digital.
- Entidades educativas y de investigación.

El alcance de la certificación podrá definirse como Organizacional (Global), abarcando a toda la entidad, o Específico (Parcial), limitado a procesos, servicios, sistemas de

información o unidades de negocio claramente delimitados. Esta flexibilidad permite una adopción progresiva y proporcional al perfil de riesgo y la estructura de cada organización.

3. Objetivos del Sello DataTrust

La misión del **Sello DataTrust Noblesse** es servir como un catalizador para la mejora de la postura de seguridad y privacidad en el ecosistema digital. Sus objetivos estratégicos se articulan en los siguientes puntos:

1. **Garantizar la Protección de la Información:** Asegurar que los activos de información estén protegidos contra accesos no autorizados, alteración, destrucción o divulgación, mediante la implementación de controles técnicos y administrativos alineados con los principios de la tríada CID (Confidencialidad, Integridad, Disponibilidad).
2. **Asegurar el Cumplimiento Normativo:** Establecer un marco que facilite el cumplimiento de un ecosistema regulatorio complejo, incluyendo, pero no limitado a, el GDPR, LGPD, CCPA, así como estándares internacionales como ISO/IEC 27001, ISO/IEC 27701, y el marco NIST Cybersecurity.
3. **Promover la Transparencia y la Ética:** Fomentar prácticas transparentes en la gestión de datos personales, asegurando que los titulares puedan ejercer efectivamente sus derechos (ARCO/PARC y otros análogos) y que el tratamiento de datos se realice bajo principios de licitud, lealtad y minimización.
4. **Mitigar Riesgos Operativos y Reputacionales:** Reducir la probabilidad e impacto de incidentes de seguridad que puedan derivar en sanciones legales, pérdidas financieras o daños a la reputación corporativa.
5. **Instaurar una Cultura de Mejora Continua:** Impulsar un ciclo perpetuo de evaluación, implementación, revisión y mejora de los controles de seguridad y privacidad, adaptándose de forma proactiva a la evolución del panorama de amenazas.

4. Principios Rectores

La certificación se fundamenta en los siguientes principios rectores, que constituyen la base filosófica de todos sus requisitos:

- **Transparencia:** Las organizaciones deben mantener una comunicación clara, accesible y veraz sobre sus políticas, prácticas y controles relacionados con la seguridad y privacidad de los datos hacia todas las partes interesadas.
- **Responsabilidad:** Se debe establecer y documentar una estructura de gobierno clara que asigne roles, responsabilidades y rendición de cuentas específicos en materia de ciberseguridad y privacidad en todos los niveles de la organización.
- **Evidencia Objetiva:** Toda afirmación de cumplimiento debe estar sustentada por evidencia objetiva, verificable y reproducible, obtenida a través de registros, logs, informes de auditoría y otros artefactos documentales.
- **Enfoque Basado en Riesgos:** Las medidas de control implementadas deben ser proporcionales a los riesgos identificados, considerando la naturaleza, el alcance, el contexto y los recursos de la organización, evitando cargas innecesarias sin comprometer la eficacia.
- **Mejora Continua:** La certificación no es un estado estático, sino un proceso dinámico que exige una revisión y optimización periódica de los sistemas de gestión para responder a cambios en el entorno interno y externo.

5. Requisitos para la Certificación

El cumplimiento de la **Norma DataTrust Noblesse** exige la implementación y operación efectiva de controles en las siguientes cinco áreas críticas:

5.1. Gobierno y Gestión de la Seguridad

La organización debe establecer un marco de gobierno formal que incluya una política de seguridad de la información, un Comité de Seguridad, la designación de un Responsable de Seguridad de la Información (CISO) y/o un Delegado de Protección de Datos (DPO), y la asignación clara de responsabilidades.

5.2. Protección de Datos y Privacidad por Diseño y por Defecto

Se requiere la implementación de medidas técnicas y organizativas para garantizar el cumplimiento de los principios de privacidad desde la fase de diseño de cualquier producto o proceso. Esto incluye la realización de Evaluaciones de Impacto en la Protección de Datos (EIPD/DPIA), la gestión del consentimiento y la habilitación de canales efectivos para que los titulares ejerzan sus derechos.

5.3. Gestión de Riesgos y Controles Técnicos

La organización debe mantener un proceso sistemático de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información. Se deben implementar controles robustos, que incluyan, entre otros: gestión de accesos e identidades, cifrado de datos, seguridad perimetral y de endpoints, copias de seguridad y planes de recuperación.

5.4. Gestión de Incidentes de Seguridad y Violaciones de Datos

Es obligatorio contar con un procedimiento formalizado para la detección, reporte, análisis, respuesta y comunicación de incidentes de seguridad y violaciones de datos personales. Se deben conservar registros detallados de cada incidente y realizar pruebas periódicas del plan de respuesta.

5.5. Auditoría Interna y Evidencia Documental

La organización debe realizar auditorías internas planificadas y periódicas para verificar la conformidad con la norma. Se debe mantener un cuerpo documental actualizado y accesible que incluya políticas, procedimientos, registros de actividades, informes de auditoría y evidencias de la operación de los controles.

6. Proceso de Certificación

El proceso para la obtención del Sello DataTrust Noblesse se estructura en las siguientes fases:

1. **Solicitud y Contratación:** Presentación formal de la solicitud y firma del contrato con Noblesse SpA, definiendo el alcance de la certificación.
2. **Evaluación de Brechas (Gap Analysis):** Auditoría preliminar voluntaria para identificar desviaciones entre el estado actual de la organización y los requisitos de la norma.
3. **Implementación y Preparación:** La organización aborda las no conformidades identificadas y prepara el cuerpo de evidencia documental requerido.
4. **Auditoría de Certificación:** Un equipo de auditores independientes y cualificados, designados por Noblesse, realiza una evaluación in situ y/o remota para verificar la implementación y eficacia de todos los requisitos.

5. **Decisión y Emisión del Sello:** Tras un análisis de los hallazgos, y una vez resueltas todas las no conformidades mayores, Noblesse emite el certificado y otorga el derecho de uso del Sello DataTrust.
6. **Auditorías de Seguimiento:** Se realizan auditorías de vigilancia anuales para confirmar el mantenimiento del cumplimiento.
7. **Renovación:** Al término de la validez del certificado (3 años), se inicia un nuevo ciclo completo de auditoría de certificación.

7. Uso del Sello y Marcas Registradas

El Sello DataTrust Noblesse es una marca registrada de propiedad de Noblesse SpA. Su uso está estrictamente regulado y limitado a las organizaciones que mantengan una certificación vigente. Debe exhibirse junto con el número de licencia y las fechas de validez. Cualquier uso no autorizado, falsificación o uso engañoso del Sello será causal de revocación inmediata de la certificación y podrá dar lugar a acciones legales.

8. Compromisos Contractuales y Revocación

La relación entre Noblesse SpA y la organización certificada se rige por un contrato de servicios. Este documento establece los derechos y obligaciones de ambas partes, las condiciones de las auditorías, las tarifas y las causales específicas para la suspensión o revocación de la certificación. La organización certificada se compromete a notificar cualquier cambio significativo que pueda afectar su cumplimiento.

9. Anexos Normativos

La presente norma se complementa con una serie de anexos informativos y normativos (estos pueden ser solicitados vía mail info@noblesse.cl), que proporcionan orientación detallada e incluyen:

- Anexo A: Modelos de Políticas y Procedimientos (Seguridad, Privacidad, Gestión de Incidentes).
- Anexo B: Guía para la Implementación de un Sistema de Gestión de Riesgos.
- Anexo C: Cláusulas Contractuales Estándar y Acuerdos de Confidencialidad.

- Anexo D: Plantillas de Registro (Matriz de Riesgos, Bitácoras de Incidentes, Actas de Auditoría).
- Anexo E: Métricas e Indicadores Clave de Desempeño (KPIs) para la Medición de la Madurez.

10. Conclusión

La **Norma DataTrust Noblesse** representa un referente de excelencia en el ámbito de la ciberseguridad y la privacidad. Su adopción trasciende el mero cumplimiento regulatorio, posicionándose como una declaración estratégica de compromiso con la confianza digital. La obtención del Sello DataTrust no es un fin, sino el comienzo de un camino de mejora continua, proporcionando una ventaja competitiva sostenible y demostrando ante el mercado una gestión responsable, ética y resiliente de la información.