

Manual Integral de Operaciones, Seguridad y Continuidad

Empresa: NovaData Solutions S.A.

Documento Interno – Uso Restringido

Versión: 2.0

Fecha de Emisión: 15 de marzo de 2024

Área Responsable: Seguridad de la Información y Operaciones

Índice

1. Introducción
 2. Alcance y Objetivos
 3. Definiciones Clave
 4. Gobierno de Accesos
 5. Seguridad de la Información
 6. Uso Aceptable de Sistemas
 7. Gestión de Incidentes
 8. Continuidad del Negocio
 9. Copias de Seguridad y Recuperación
 10. Auditoría y Cumplimiento
 11. Terminación de Relación Laboral
 12. Preguntas Frecuentes (FAQ)
 13. Anexos
-

1. Introducción

Este manual establece las políticas, procedimientos y lineamientos que regulan el uso de los sistemas tecnológicos, la información y los recursos digitales de **NovaData Solutions S.A.**

Su cumplimiento es **obligatorio** para:

- Empleados
- Contratistas
- Proveedores tecnológicos

- Personal temporal con acceso a sistemas internos

El desconocimiento de este documento **no exime de responsabilidad**.

2. Alcance y Objetivos

2.1 Alcance

Aplica a todos los sistemas:

- Infraestructura cloud
- Sistemas internos
- Bases de datos
- Herramientas colaborativas
- Dispositivos corporativos

2.2 Objetivos

- Proteger la información confidencial
 - Garantizar la continuidad operativa
 - Reducir riesgos operativos y legales
 - Establecer responsabilidades claras
-

3. Definiciones Clave

- **Información Confidencial:** Datos no públicos cuya divulgación puede causar daño.
 - **Incidente de Seguridad:** Evento que compromete o amenaza la seguridad.
 - **MFA:** Autenticación multifactor.
 - **Backup:** Copia de seguridad de datos.
 - **Usuario:** Persona con acceso autorizado a sistemas.
-

4. Gobierno de Accesos

4.1 Principio de Mínimo Privilegio

Cada usuario debe tener **solo los accesos estrictamente necesarios** para cumplir su función.

4.2 Credenciales

- Las credenciales son personales e intransferibles.
- Las contraseñas deben:
 - Tener al menos 12 caracteres
 - Incluir mayúsculas, minúsculas y números
- Cambio obligatorio cada **90 días**.

4.3 Autenticación Multifactor (MFA)

El MFA es obligatorio para:

- Accesos remotos
- Accesos administrativos
- Sistemas críticos

Métodos permitidos:

- Aplicación autenticadora
 - Token físico
 - SMS (solo como contingencia)
-

5. Seguridad de la Información

5.1 Clasificación de la Información

La información se clasifica como:

- Pública
- Interna
- Confidencial
- Crítica

5.2 Almacenamiento Seguro

- La información confidencial debe almacenarse cifrada.
- Está prohibido usar servicios personales (ej. Google Drive personal).

5.3 Transmisión de Datos

- Solo se permiten canales cifrados (HTTPS, VPN).

- No se permite enviar datos sensibles por correo sin cifrado.
-

6. Uso Aceptable de Sistemas

Los sistemas deben usarse **exclusivamente para fines laborales**.

No está permitido:

- Instalar software no autorizado
 - Compartir cuentas
 - Intentar evadir controles de seguridad
 - Usar sistemas para fines ilegales o personales graves
-

7. Gestión de Incidentes

7.1 Definición de Incidente

Se considera incidente cualquier evento que:

- Exponga información
- Interrumpa servicios
- Vulnere controles de seguridad

7.2 Reporte de Incidentes

Todo incidente debe reportarse **dentro de las primeras 2 horas**.

Información mínima:

- Fecha y hora
- Sistemas afectados
- Descripción del incidente
- Usuario que detectó el evento

7.3 Respuesta Inicial

El equipo de seguridad podrá:

- Revocar accesos
- Aislar sistemas
- Ejecutar análisis forense

8. Continuidad del Negocio

8.1 Objetivo

Garantizar la operación ante fallas técnicas, incidentes o desastres.

8.2 Escenarios Cubiertos

- Fallas de infraestructura
- Ataques cibernéticos
- Errores humanos
- Cortes de energía

9. Copias de Seguridad y Recuperación

9.1 Frecuencia

- Backups incrementales: diarios
- Backups completos: semanales
- Backups mensuales: archivo histórico

9.2 Retención

- Backups diarios: 30 días
- Backups semanales: 3 meses
- Backups mensuales: 12 meses

9.3 Pruebas

Los backups deben probarse **al menos una vez por trimestre**.

10. Auditoría y Cumplimiento

La empresa se reserva el derecho de:

- Auditar accesos
- Revisar logs
- Verificar cumplimiento de políticas

El incumplimiento puede resultar en sanciones disciplinarias.

11. Terminación de Relación Laboral

Al finalizar la relación laboral:

- Se revocarán accesos el mismo día
- Se devolverán dispositivos
- Se realizará una auditoría básica

12. Preguntas Frecuentes (FAQ)

¿Cada cuánto debo cambiar mi contraseña?

Cada 90 días.

¿Qué hago si pierdo mi token MFA?

Reportarlo inmediatamente al equipo de seguridad.

¿Puedo usar mi correo personal?

No, salvo autorización explícita.

13. Anexos

Anexo A – Contactos

- Seguridad de la Información: seguridad@novadata.com
- Soporte Técnico: soporte@novadata.com

Anexo B – Historial de Cambios

- v1.0 – Enero 2023
- v1.5 – Julio 2023
- v2.0 – Marzo 2024