#### Roberto Blanco

### Clasificación de la Información

## Categorías:

- **Confidencial:** Incluye información altamente sensible como datos financieros, contratos legales, credenciales de sistemas, datos personales de clientes y empleados.
- **Restringida:** Comprende información técnica o de uso interno como código fuente, manuales de operación, documentación de proyectos, reportes internos.
- Pública: Información que puede ser divulgada sin afectar a la empresa, como el contenido del sitio web, material de marketing y publicaciones oficiales.

## Propósito:

Garantizar que la información sea manejada y protegida conforme a su nivel de sensibilidad, evitando accesos no autorizados y aplicando controles adecuados según su clasificación.

#### 7. Control de Acceso

### Medidas implementadas:

- Autenticación Multifactor (MFA): Todos los usuarios deben autenticarse usando al menos dos métodos (por ejemplo, contraseña + código por aplicación móvil).
- Revisión periódica de permisos: Cada 6 meses se realiza una auditoría para verificar que los usuarios solo tengan los permisos necesarios para su rol.
- Registro de accesos fallidos: Se habilita un sistema de registros (logs) que documenta todos los intentos fallidos de acceso para detectar actividades sospechosas.

# Propósito:

Limitar el acceso a los recursos en función de los roles y responsabilidades de los empleados, reduciendo el riesgo de violaciones por privilegios innecesarios o mal uso de credenciales.

## 8. Gestión de Incidentes de Seguridad

# **Acciones propuestas:**

- Flujo de respuesta a incidentes:
  - 1. Detección y notificación inmediata del incidente.
  - 2. Clasificación del tipo y nivel de impacto.
  - 3. Contención y mitigación del incidente.
  - 4. Investigación y análisis de causa raíz.
  - 5. Documentación y aprendizaje.

# Formulario de reporte de incidentes:

Incluye campos como tipo de incidente (p. ej., acceso no autorizado, malware), fecha y hora, área afectada, persona que reporta, descripción del evento, y acciones tomadas.

### **Propósito:**

Asegurar una respuesta eficiente y estructurada ante eventos de seguridad, minimizando el impacto y permitiendo la mejora continua del sistema.

# 9. Política de Uso Aceptable

#### **Directrices establecidas:**

- Actividades permitidas: Uso del correo electrónico institucional, acceso a sistemas autorizados, navegación en sitios relacionados con el trabajo.
- Actividades prohibidas: Instalación de software no autorizado, acceso a contenido inapropiado o ilegal, uso de dispositivos personales sin autorización, compartir contraseñas.

### Propósito:

Fomentar el uso responsable de los recursos tecnológicos de la empresa, garantizando que su utilización no comprometa la seguridad ni el funcionamiento de los sistemas.

# 10. Gestión de Riesgos

### **Acciones implementadas:**

- Formulario de evaluación de riesgos: Para identificar y calificar amenazas, vulnerabilidades, impacto y probabilidad.
- Riesgos críticos identificados:
  - 1. Acceso no autorizado a información sensible.
  - 2. Pérdida de datos por fallos técnicos.
  - 3. Ataques de malware/ransomware.
  - 4. Errores humanos por falta de capacitación.
  - 5. Fallos en proveedores externos.

# Planes de mitigación:

- o Implementación de copias de seguridad automáticas.
- Aplicación de controles de acceso.
- o Programas de capacitación.
- o Auditoría a proveedores.
- Monitoreo continuo de amenazas.