Política de Seguridad de la Información - Bloque 3

# 11. Formación y Concienciación

La organización establece un programa anual de formación en seguridad de la información, obligatorio para todo el personal. Este programa tiene como objetivo garantizar que los empleados comprendan los riesgos asociados al manejo de la información y adopten comportamientos seguros en sus funciones diarias.  
  
El cronograma de formación contempla:  
- Capacitaciones semestrales sobre amenazas digitales emergentes, como phishing, ransomware e ingeniería social.  
- Simulaciones trimestrales de ataques de phishing, con métricas de desempeño. Se espera que al menos el 85% del personal identifique correctamente intentos maliciosos.  
- Distribución de materiales educativos como guías de buenas prácticas en contraseñas, navegación segura y uso adecuado del correo electrónico corporativo.  
  
El área de Seguridad de la Información llevará un registro de asistencia y resultados de cada sesión, además de aplicar evaluaciones para medir la efectividad de la capacitación.

# 12. Gestión de Proveedores

Los proveedores que tengan acceso a información sensible o sistemas críticos de la empresa deberán cumplir con los requisitos establecidos en esta Política de Seguridad.  
  
Todos los contratos incluirán cláusulas específicas que obligan a los proveedores a:  
- Cifrar datos sensibles tanto en tránsito como en reposo.  
- Aplicar controles de acceso según el principio de menor privilegio.  
- Notificar de inmediato cualquier incidente de seguridad que pueda comprometer los activos de la empresa.  
  
Además, la empresa realizará una evaluación inicial de seguridad antes de establecer relaciones comerciales, y llevará a cabo auditorías anuales para validar el cumplimiento continuo. Los resultados de estas evaluaciones influirán en la renovación o cancelación de contratos.

# 13. Revisión y Auditoría

Para garantizar la mejora continua de la política de seguridad de la información, se establecen los siguientes mecanismos de revisión:  
  
- Se realizarán auditorías internas cada seis meses, enfocadas en verificar la aplicación de controles técnicos y procedimientos administrativos.  
- Durante las auditorías se revisarán configuraciones de firewalls, registros de accesos, políticas de respaldo, y cumplimiento con las capacitaciones obligatorias.  
- Los hallazgos serán documentados en informes oficiales y compartidos con la alta dirección. Cada hallazgo deberá tener un plan de acción asignado con plazos definidos y responsables claros.  
  
Este proceso permitirá identificar desviaciones, corregirlas oportunamente y mantener la alineación con las mejores prácticas internacionales.

# 14. Consecuencias del Incumplimiento

El incumplimiento de esta Política de Seguridad será tratado con seriedad y conforme a la gravedad del caso. Las consecuencias se aplicarán de manera progresiva:  
  
- Primera infracción: Advertencia escrita con explicación de la política vulnerada.  
- Segunda infracción: Suspensión temporal del acceso a los sistemas corporativos por un período de tres días laborables.  
- Tercera infracción o incumplimiento grave: Evaluación disciplinaria que puede culminar en la terminación del contrato laboral.  
  
Las sanciones serán documentadas en el expediente del colaborador. El empleado tendrá derecho a presentar una apelación formal ante el Comité de Seguridad o Recursos Humanos.

# 15. Referencias

Esta política se ha desarrollado considerando los siguientes marcos regulatorios y normativos:  
  
- ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI).  
- ISO/IEC 27002: Código de buenas prácticas para controles de seguridad.  
- Ley de Protección de Datos Personales (según legislación local).  
- Ley Nacional sobre Delitos Informáticos, aplicable a incidentes de seguridad y manejo indebido de la información.  
- Manuales internos de privacidad, continuidad del negocio y uso aceptable de recursos.