BPIC
A Member-Owned Insurance Company

Bishops' Plan Insurance Company

Noticias sobre seguridad y control de pérdidas

Preparado por Gallagher Bassett | Servicios de control de riesgos *Principios de la primavera 2026*

En este número:

Sobre BPIC

Bishops' Plan Insurance Company (BPIC) es una sociedad cautiva y colaborativa sin fines de lucro, con domicilio en Vermont, que agrupa a las diócesis y arquidiócesis del Directorio Kenedy, creada en 2003 para atender sus necesidades de financiación y gestión de riesgos. Somos 33 miembros repartidos por todo el país. BPIC ofrece una estructura personalizable y ofertas de beneficios que permiten a cada diócesis trabajar con su corredor y el equipo de suscripción de BPIC en el diseño de su propia estructura de programa, utilizando las capacidades únicas de todas las líneas del programa. BPIC está dirigida por su junta directiva junto con la orientación espiritual de su moderador episcopal y varios proveedores de servicios asociados externos. BPIC ofrece un sitio web exclusivo para miembros (protegido por contraseña) que incluye información financiera de la empresa y recursos de gestión de riesgos. Si desea más información sobre BPIC o nuestro sitio web, a continuación encontrará la información de contacto.

Teléfono
Número gratuito: 877.325.PBIC (2742)

Correo electrónico:
info@bpicmembers.org

Sitio web:
www.bpicmembers.org

Preparación de las instalaciones para la primavera: una lista de verificación para después del invierno

A medida que las heladas invernales comienzan a derretirse y se asoma la promesa de la primavera, las instalaciones deben prepararse para la transición estacional. El clima invernal puede afectar los edificios, los terrenos y los equipos, y abordar estos problemas de manera temprana garantiza que las instalaciones sigan siendo seguras, funcionales y acogedoras para los feligreses y el personal. Una preparación adecuada también contribuye a prevenir reparaciones costosas y garantiza que las instalaciones estén listas para la activa temporada de primavera, que suele incluir celebraciones de Pascua, eventos al aire libre y reuniones comunitarias.

A continuación, se presenta una guía integral para ayudar a las diócesis a preparar sus instalaciones para la primavera después de la temporada invernal:

1. Inspeccionar y reparar los exteriores del edificio

El clima invernal puede causar un desgaste significativo en el exterior de una instalación. Comience con una inspección minuciosa:

- **Techo:** compruebe si hay tejas faltantes, dañadas o sueltas, así como señales de filtraciones o daños por agua. Aborde cualquier problema de inmediato para evitar otros daños durante las lluvias de primavera.
- **Canaletas y bajantes pluviales:** retire residuos como hojas, hielo y suciedad para garantizar un drenaje adecuado. Compruebe que los bajantes pluviales dirijan el agua lejos de los cimientos del edificio.
- **Revestimiento y paredes:** busque grietas, pintura descascarada u otros daños causados por temperaturas bajo cero o humedad.
- **Puertas y ventanas:** inspeccione los sellos y burletes para asegurarse de que permanezcan intactos y sean eficaces desde el punto de vista energético.

2. Evaluar y mantener el espacio exterior

El invierno puede dejar los espacios al aire libre con un aspecto descuidado. Prepare los terrenos para la primavera:

- **Retirando residuos:** deshágase de ramas caídas, hojas y otros residuos de zonas de césped, jardines y senderos.
- **Realizando tareas de poda y recorte:** pode las ramas muertas o dañadas de árboles y arbustos para fomentar un crecimiento saludable y prevenir riesgos.
- **Cuidando el césped:** airee y fertilice el césped para fomentar un nuevo crecimiento. Vuelva a sembrar las zonas que quedaron al descubierto por la nieve o el hielo.
- **Probando los sistemas de riego:** pruebe los sistemas de aspersores para asegurarse de que funcionen correctamente y repare cualquier fuga o daño causado por temperaturas bajo cero.

3. Inspeccionar estacionamientos y senderos

La nieve, el hielo y la sal pueden causar grietas y baches en las superficies pavimentadas. Aborde estos problemas para garantizar la seguridad y la accesibilidad:

- **Reparar los baches:** rellene los baches y las grietas en los estacionamientos y accesos vehiculares para evitar un mayor deterioro.
- **Limpiar los senderos:** lave con hidrolavadora las aceras y entradas para deshacerse de residuos de sal y suciedad.
- **Volver a pintar las señalizaciones:** renueve las líneas desvanecidas del estacionamiento, los espacios para personas con discapacidad y las flechas direccionales.

(Continúa en la página 2)

Preparación de las instalaciones para la primavera: una lista de verificación para después del invierno

(Continúa de la página 1)

4. Dar mantenimiento a los sistemas de HVAC

A medida que aumentan las temperaturas, es fundamental asegurarse de que los sistemas de calefacción, ventilación y aire acondicionado (HVAC) estén listos para los meses más cálidos:

- **Cambiar al modo de refrigeración:** pruebe las unidades de aire acondicionado para asegurarse de que funcionen correctamente.
- **Reemplazar los filtros:** limpie o reemplace los filtros del sistema de HVAC para mejorar la calidad del aire y la eficacia del sistema.
- **Programar tareas de mantenimiento:** solicite a un profesional que inspeccione y realice el mantenimiento del sistema de HVAC para abordar cualquier problema antes de su uso intensivo.

5. Revisar los sistemas de plomería

Las temperaturas bajo cero pueden hacer que las tuberías se agrieten o revienten. Inspeccione los sistemas de plomería en busca de cualquier señal de daño:

- **Inspeccionar las tuberías:** busque fugas, grietas o corrosión en las tuberías expuestas.
- **Probar grifos exteriores:** abra los grifos exteriores para asegurarse de que el agua fluya libremente y compruebe si hay fugas.
- **Revisar calentadores de agua:** asegúrese de que los calentadores de agua funcionen correctamente y ajuste la temperatura si es necesario para un clima más cálido.

6. Limpiar bien los espacios interiores

La primavera es el momento perfecto para realizar una limpieza exhaustiva del interior de la instalación:

- **Desinfectar las áreas comunes:** limpie y desinfecte las superficies de alto contacto, como manijas de puertas, interruptores de luz y bancos.
- **Limpiar las ventanas:** elimine la suciedad y la mugre de las ventanas para que entre más luz natural.
- **Limpiar los pisos y las alfombras:** realice una limpieza profunda de las alfombras y pula los pisos duros para eliminar la suciedad y los residuos de sal del invierno.
- **Ordenar las áreas de almacenamiento:** organice y limpie los espacios de almacenamiento para prepararse para los próximos eventos y actividades.

7. Probar los sistemas de seguridad y protección

Asegúrese de que se hayan implementado todas las medidas de seguridad y protección y de que funcionen:

- **Seguridad contra incendios:** pruebe los detectores de humo, las alarmas contra incendios y los sistemas de rociadores. Reemplace las baterías y programe inspecciones si es necesario.
- **Salidas de emergencia:** compruebe que todas las salidas de emergencia estén despejadas y bien señalizadas.
- **Sistemas de seguridad:** pruebe las cámaras de seguridad, las alarmas y los sistemas de control de acceso para asegurarse de que funcionen.

8. Planificar los eventos de primavera

La primavera es una época activa para las organizaciones diocesanas, con eventos como servicios de Pascua, reuniones al aire libre y programas de alcance comunitario. Prepárese:

- **Programando las tareas de mantenimiento:** realice todas las reparaciones y tareas de limpieza necesarias antes de los eventos principales.
- **Acondicionando los espacios exteriores:** organice los asientos, las tiendas y las decoraciones para servicios o actividades al aire libre.
- **Abasteciendo suministros:** asegúrese de contar con suficientes productos de limpieza, desinfectantes para manos y otros artículos esenciales.

9. Comunicarse con el personal y los voluntarios

Involucre al personal y a los voluntarios en el proceso de preparación:

- **Asignar tareas:** cree una lista de verificación de tareas y delegue responsabilidades para garantizar que todo se realice a tiempo.
- **Brindar capacitación:** ofrezca orientación sobre los procedimientos adecuados de limpieza, mantenimiento y seguridad.
- **Fomentar los comentarios:** solicite aportes del personal y los voluntarios sobre áreas que puedan necesitar atención.

10. Presupuestar reparaciones y mejoras

El mantenimiento de primavera es una oportunidad para abordar no solo reparaciones inmediatas, sino también mejoras a largo plazo:

- **Evaluar las necesidades:** evalúe el estado de la instalación y priorice los proyectos según la urgencia y el presupuesto.
- **Planificar las mejoras:** considere mejoras que sean eficaces desde el punto de vista energético, como iluminación LED o paneles solares, para reducir los costos de servicios públicos y el impacto ambiental.

Conclusión

Preparar las instalaciones diocesanas para la primavera es una parte fundamental de la buena administración, que garantiza que los edificios y terrenos permanezcan seguros, acogedores y funcionales para la comunidad. Al abordar los daños relacionados con el invierno, realizar las tareas de mantenimiento de rutina y planificar los próximos eventos, las diócesis pueden crear un entorno dinámico y acogedor para feligreses y visitantes por igual. Con un poco de esfuerzo y organización, sus instalaciones estarán listas para abrazar la belleza y la renovación de la temporada de primavera.

Regrese al En este número.

Capacitación del personal en ciberseguridad

Capacitar al personal en ciberseguridad es una de las formas más eficaces de proteger su organización contra las amenazas cibernéticas. Al dotar a empleados y voluntarios de los conocimientos y las habilidades para reconocer y responder posibles riesgos, puede crear una sólida primera línea de defensa. Considere adoptar las siguientes medidas prácticas para capacitar al personal en ciberseguridad.

Realizar capacitaciones periódicas de concientización en ciberseguridad

- **Frecuencia:** programe sesiones de capacitación al menos dos veces al año o cada vez que haya actualizaciones significativas en los protocolos de ciberseguridad.
- **Contenido:** cubra temas como el reconocimiento de correos electrónicos de *phishing*, la creación de contraseñas seguras, la navegación segura por Internet y el manejo de datos sensibles.
- **Aprendizaje interactivo:** recurra a cuestionarios, situaciones de juego de roles y ejemplos de la vida real para que la capacitación sea atractiva e inolvidable.

Enseñar al personal a reconocer amenazas cibernéticas comunes

- **Correos electrónicos de *phishing*:** muestre ejemplos de correos electrónicos falsos y enseñe al personal a identificar señales de alerta como errores ortográficos, enlaces sospechosos o solicitudes urgentes de información personal.
- **Ingeniería social:** explique cómo los atacantes pueden utilizar tácticas de manipulación para poder acceder a información sensible.
- ***Malware* y *ransomware*:** eduque al personal sobre cómo el *software* malicioso puede infectar los sistemas y cómo evitar descargar archivos sospechosos o hacer clic en enlaces desconocidos.

Implementar simulacros de ciberseguridad

- Realice campañas simuladas de *phishing* para poner a prueba la capacidad del personal a la hora de identificar y denunciar correos electrónicos sospechosos.
- Utilice estos simulacros como oportunidades de aprendizaje para reforzar las mejores prácticas y abordar cualquier brecha de conocimiento.

Proporcionar políticas y directrices claras

- Elabore y distribuya una política de ciberseguridad que describa el uso aceptable de la tecnología, los requisitos de contraseñas y los procedimientos para denunciar incidentes.
- Asegúrese de que el personal comprenda la importancia de cumplir con estas políticas y las consecuencias de no cumplirlas.

Realice campañas simuladas de *phishing* para poner a prueba la capacidad del personal a la hora de identificar y denunciar correos electrónicos sospechosos.

Promover el uso de contraseñas seguras y autenticación de múltiples factores (MFA)

- Enseñe al personal cómo crear contraseñas seguras y únicas utilizando una combinación de letras, números y símbolos.
- Fomente el uso de gestores de contraseñas para almacenar y administrar contraseñas de forma segura.
- Capacite al personal sobre cómo configurar y utilizar la MFA como una capa extra de seguridad.

Destacar la importancia de la protección de datos

- Explique la importancia de proteger información sensible, como registros de feligreses, datos financieros y comunicaciones internas.
- Capacite al personal en prácticas seguras de intercambio de archivos y en la importancia de cifrar datos sensibles.

Proporcionar recursos y actualizaciones de forma continua

- Comparta consejos y actualizaciones de ciberseguridad a través de boletines, correos electrónicos o tableros informativos.
- Ofrezca acceso a cursos en línea, seminarios web o talleres sobre temas de ciberseguridad.
- Mantenga al personal informado sobre amenazas emergentes y cómo responder a estas.

(Continúa en la página 4)

Capacitación del personal en ciberseguridad

(Continúa de la página 3)

Designar un referente de ciberseguridad

- Designe a un miembro del personal o a un equipo para que actúe como recurso principal para preguntas e inquietudes relacionadas con la ciberseguridad.
- Esta persona también puede supervisar el cumplimiento, proporcionar capacitación extra y mantenerse actualizada sobre las últimas tendencias en ciberseguridad.

Fomentar una cultura de denuncias

- Capacite al personal para que denuncie correos electrónicos, enlaces o actividades sospechosas de inmediato, sin temor a represalias.
- Establezca un proceso sencillo y claro para denunciar posibles incidentes de ciberseguridad.

Asociarse con expertos en ciberseguridad

- Invite a profesionales externos en ciberseguridad para realizar talleres o brindar una capacitación especializada.
- Considere asociarse con organizaciones que ofrezcan capacitación en ciberseguridad adaptada a organizaciones religiosas o sin fines de lucro.

Evaluar y mejorar los programas de capacitación

- Recopile comentarios del personal después de cada sesión de capacitación para identificar áreas de mejora.
- Evalúe periódicamente la eficacia de su programa de capacitación mediante encuestas, pruebas o ataques simulados.

Predicar con el ejemplo

- El liderazgo debe modelar buenas prácticas de ciberseguridad, como utilizar contraseñas seguras, denunciar actividades sospechosas y respetar las políticas organizacionales.
- Cuando el personal ve que los líderes priorizan la ciberseguridad, es más probable que se la tome en serio.

Conclusión

Capacitar al personal en ciberseguridad es un proceso continuo que exige compromiso y constancia. Al invertir en educación y fomentar una cultura de control, su organización diocesana puede reducir significativamente el riesgo de ciberataques. Recuerde que la ciberseguridad es una responsabilidad compartida, y cada miembro del personal desempeña un papel fundamental a la hora de proteger la organización y su comunidad. Juntos, podemos construir un entorno digital más seguro para todos.

Amenazas cibernéticas comunes

Ataques de phishing

Se trata de correos electrónicos o mensajes fraudulentos diseñados para engañar a las personas y hacer que revelen información sensible, como contraseñas o datos financieros.

Ransomware

Se trata de un software malicioso que bloquea el acceso a sistemas o datos hasta que se paga un rescate.

Violaciones de datos

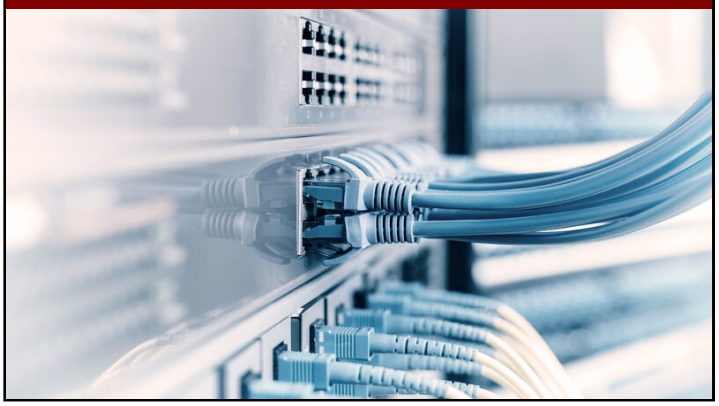
Se trata del acceso no autorizado a información sensible, que suele dar como resultado la exposición de datos personales o financieros.

Ingeniería social

Se trata de tácticas manipuladoras utilizadas por ciberdelincuentes para engañar a las personas y hacer que divulguen información confidencial.

Contraseñas débiles

Se trata de contraseñas fáciles de adivinar o que se vuelven a utilizar que facilitan a los hackers el acceso a los sistemas.



Regrese al En este número.