POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE MANPOWERGROUP

CONTEXTO ACTUAL: TRANSFORMACIÓN DIGITAL RÁPIDA

La gravedad, la frecuencia y el impacto de los delitos cibernéticos ha ido en aumento durante varios años. Ahora, con la aceleración del trabajo remoto y la rápida digitalización, las organizaciones requerirán una priorización aún mayor de las capacidades de seguridad de la información. Los líderes empresariales y de seguridad se enfrentan a desafíos de velocidad operativa avanzada, resistencia sin precedentes y una creciente supervisión regulatoria.

A medida que la tecnología evoluciona y adoptamos nuevas herramientas y ampliamos nuestro uso de datos y análisis para ofrecer más valor a los clientes y candidatos, nos comprometemos a ser buenos administradores de la información que se nos confía. Administrar nuestra seguridad de la información es vital para garantizar la confianza y la transparencia con nuestros empleados, clientes, candidatos, asociados y socios. Al mismo tiempo, la frecuencia y la sofisticación de los ataques cibernéticos están aumentando y asumimos nuestra responsabilidad de estar atentos y educar seriamente a nuestra gente.

Randy L. Herold
Director de Seguridad de la Información y Director de Privacidad

NUESTRA PRINCIPIOS RECTORES

Mantener la información segura requiere una evaluación de riesgos constante. Nuestro Programa de Seguridad y Privacidad de la Información es un marco global que va más allá de los conjuntos de herramientas preventivas, combinando personas, procesos y tecnología para reducir riesgos y crear valor para nuestros clientes. Nuestra principal prioridad es proteger los datos que las personas nos confían.

Nuestro compromiso con los más altos estándares de seguridad de la información y privacidad de datos se describe en nuestro Código Global de Conducta Empresarial y Ética. Disponible en 20 idiomas, nuestro Código se comparte con todos los empleados y puede estar disponible para nuestros grupos deinterés en todo el mundo.

GENTE

• Reconocer que la mejor línea de defensa no es una herramienta ni plataforma, es nuestra gente.

• Comprender e influir en el comportamiento del usuario mediante saber dónde reside la información, cómo se mueve a través de nuestros sistemas y quién tiene acceso a ella durante todo el ciclo de vida de la información, para que podamos proteger los datos de nuestros empleados, clientes, candidatos, asociados y terceros.

• Aprovechar la inteligencia colectiva de amenazas a través de relaciones con socios de la industria como el FS ISAC, lo que nos permite compartir prácticas y maximizar nuestras capacidades de seguridad

PROCESOS

• Posicionar la seguridad de la información como un Órgano rector - la seguridad de la información proporciona la supervisión necesaria para alinear nuestros servicios de tecnología con los requisitos comerciales, legales y reglamentarios.

• Centrarse en el conocimiento/conciencia de la situación y el tiempo de respuesta orientando nuestras capacidades de monitoreo específicamente hacia formas en que podemos mejorar nuestra conciencia.

TECNOLOGÍA

• Reconociendo que la tecnología preventiva no es suficiente para mantener a raya a un atacante determinado, hemos ampliado nuestras capacidades de detección y respuesta en toda la organización.

• Prevención del robo de credenciales al priorizar capacidades de gestión de acceso privilegiado.

GENTE

PROTEGIENDO LO QUE IMPORTA:

NUESTROS EMPLEADOS, CLIENTES Y ASOCIADOS

En ManpowerGroup, nuestro impacto se extiende mucho más allá de nuestras propias operaciones internas. Nuestros clientes y asociados nos confían sus datos empresariales confidenciales, y nos tomamos esa responsabilidad seriamente. Nuestra Política de Privacidad Global describe los tipos de información personal que recopilamos de empleados, clientes, candidatos, asociados y terceros, cómo la usamos, con quién la compartimos y los derechos y opciones disponibles para las personas con respecto a nuestro uso de su información. Todas las políticas de privacidad, mantenidas a nivel de país, se alinean con nuestros estándares globales y cumplen con las leyes y regulaciones locales.

LIDERANDO DESDE LA CIMA

Nuestra filosofía de seguridad de la información está liderada desde arriba con la capacidad de supervisión de nuestra Junta para garantizar que las principales amenazas a la seguridad se gestionen a través de una estructura de gobierno y gestión eficaz. El Director de Seguridad de la Información (CISO) se reúne trimestralmente con el Comité de Auditoría de la Junta Directiva para revisar y discutir la estrategia de seguridad y el progreso en torno a nuestras inversiones. Bajo la dirección del CISO, la responsabilidad de nuestro programa de seguridad global reside en los niveles más altos de liderazgo ejecutivo que reportan al Director Financiero.

UN ENFOQUE DE GOBERNANZA DE MÚLTIPLES CAPAS

Mientras nuestro CISO mantiene una cadencia regular de informes con la Junta Directiva de ManpowerGroup, incluido un informe anual que describe nuestro cumplimiento y adhesión a esta Política de seguridad de la información, la función de Seguridad opera independientemente de la Tecnología de la información (TI). Se proporcionan actualizaciones periódicas tanto a la Junta como al Equipo de Liderazgo Ejecutivo, así como a varios comités directivos y de trabajo. El Programa de seguridad de la información es evaluado anualmente por un tercero independiente para garantizar la alineación con el panorama de amenazas actual.

Nuestra estructura organizacional utiliza un enfoque funcional donde la estrategia, la alineación comercial y la supervisión son responsabilidades directas del CISO. Las funciones, como la arquitectura, las operaciones y la gestión de proveedores, residen en el equipo de informes directos del CISO, que incluye contratistas externos y proveedores de servicios gestionados.

Nuestro talentoso equipo dedicado a la seguridad de la información y la privacidad de los datos ha aumentado significativamente en tamaño en los últimos años. Nuestra gente está estratégicamente posicionada a nivel de mercado global, regional y local para proporcionar políticas, procesos y soluciones tecnológicas coherentes. Nuestro personal altamente capacitado mantiene certificaciones de la industria que incluyen: CISSP, CISM, CISA, CRISC, CSCP, CCISO, CCSP, CASP, CPDSE, Auditor líder ISO 27001, Gerente de riesgos ISO/IEC 27005, CIPM, CIPP/E, FIP.

DESARROLLANDO DE LAS CAPACIDADES Y HABILIDADES DE NUESTRA GENTE

Reconocemos que la tecnología preventiva no es suficiente para mantener a raya a un adversario determinado y reconocemos que nuestra mejor línea de defensa contra las amenazas a la seguridad no es una herramienta o plataforma tecnológica: es nuestra gente.

Por eso, desarrollamos continuamente programas actualizados de educación y concienciación de los empleados, que incluyen formación en línea, ejercicios periódicos contra lel phshing y la campaña del Mes Cibernético en toda la empresa, que ofrece formación diaria, seminarios dirigidos por instructores, actividades en equipo y pruebas y concursos relacionados con la seguridad. Todos los miembros del equipo de dirección ejecutiva participan en todas las campañas de formación cibernética y concienciación sobre suplantación de identidad junto con toda la organización. A través de esta formación de concienciación, se enseña a los empleados cómo informar de actividades sospechosas que identifiquen en su entorno de trabajo o en la tecnología que utilizan. Por ejemplo, la perfecta integración de la seguridad permite a los empleados informar de correos electrónicos sospechosos de phishing con un solo clic. Además, los proveedores de servicios externos y los socios con acceso a datos o sistemas confidenciales deben participar en una formación de concienciación sobre seguridad equivalente a la que que se imparte a los empleados de ManpowerGroup.

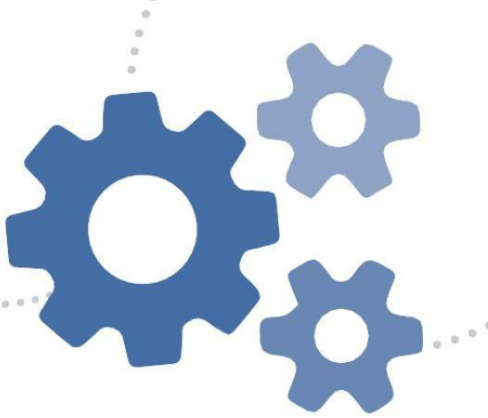
A través de estos esfuerzos de concientización mejorados y específicos, el compromiso de los empleados y las campañas de aprendizaje digital, y las comunicaciones periódicas de los equipos de seguridad de la información y CISO, estamos fomentando una cultura consciente de los riesgos en toda nuestra organización y nuestra resistencia a la ingeniería social sigue mejorando año tras año.

Incoporando la seguridad en nuestras prácticas de personas y cultura

ManpowerGroup garantiza que las prácticas de seguridad reconocidas por la industria se incorporen a nuestras Prácticas de gestión de empleados de Personas y Cultura (P&C), que incluyen:

- Definir, documentar y comunicar los roles de seguridad de la información y responsabilidades de los empleados, contratistas y usuarios externos a través del programa de concientización sobre seguridad
- Firmar acuerdos de confidencialidad como parte de un contrato de trabajo
- Exigir a terceros que mantengan el cumplimiento de los requisitos de seguridad de la información
- Garantizar que los empleados tengan acceso a las políticas, normas y procedimientos de seguridad actuales
- Brindar a los empleados, incluidos los líderes ejecutivos y CISO, capacitación periódica sobre concientización de seguridad de lainformación.
- Garantizar que los activos de información de ManpowerGroup se devuelvan al finalizar el contrato
- Eliminación de los derechos de acceso a la información al finalizar el compromiso

PROCESOS



PROTOCOLO DE MANTENIMIENTO

Hemos establecido un framework integral de seguridad de la información global, alineado con el NIST CSF (National Institute of Standars and Technology Cyber Security Framework) y el estándar ISO 27001 reconocido internacionalmente, que todas nuestras operaciones en todo el mundo deben adoptar. Todas las políticas, procedimientos, controles y estándares han sido documentados, comunicados y operacionalizados; cada uno tiene un propietario dedicado y se revisan al menos una vez al año para verificar su idoneidad y adecuación. ManpowerGroup utiliza múltiples tecnologías, así como procesos de verificación manual para hacer cumplir las políticas internas, así como los requisitos normativos y contractuales.

Políticas: para alinearse con los estándares de la industria.

Controles: para confirmar que se aplican las políticas.

Normas/Estándares: para asegurar el cumplimiento contractual, legal y normativo.

Procedimientos: para utilizar las normas.

SEGURO, POR DISEÑO

Reconocer que la tecnología preventiva no es suficiente, todos nuestros procesos están diseñados con una filosofía de defensa en profundidad; si una capa del proceso falla, se diseña un proceso posterior para mitigar el riesgo. Los controles de seguridad son implementados en varias capas y se integran en una solución de monitoreo centralizada, lo que garantiza que podamos monitorear y responder de manera eficiente las 24 horas del día, los 7 días de la semana. A través de todos nuestros procesos, trabajamos para prevenir el robo de credenciales aprovechando los principios de "privilegio mínimo" y "necesidad de saber" para minimizar el riesgo de acceso y limitar el movimiento lateral dentro de nuestro entorno.

SUPERVISANDO LOS SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN EXTERNALIZADOS

Algunas actividades diarias de seguridad operativa se subcontratan para brindarnos acceso a nuevos conjuntos de habilidades y maximizar nuestra inversión financiera. Todos los recursos de terceros aprovechados para la experiencia en seguridad de la información se investigan antes de la contratación y deben cumplir o superar los estándares de política propios de ManpowerGroup. Para garantizar la calidad y seguridad de la información, estos proveedores están sujetos a acuerdos de nivel de servicio vinculantes contractualmente, revisiones comerciales periódicas y auditorías de sus prácticas.

Hemos establecido controles para proteger la integridad, la confidencialidad y la disponibilidad de los activos de información a los que pueden acceder subcontratistas, socios, clientes y proveedores externos, incluidos:

- Requerir que los acuerdos o contratos con terceros que creen, accedan, almacenen, transmitan y/o procesen la información de ManpowerGroup incluyan los Requisitos de Seguridad de la Información del Proveedor (VISR en inglés) definido para el tipo de servicios prestados
- Requerir la aprobación del CISO o del delegado para los cambios en los requisitos de seguridad de la información
- Requerir corrección o implementación de controles de mitigación para los riesgos de procesamiento comercial identificados por terceros.
- Garantizar que existan acuerdos de confidencialidad y no divulgación firmados o documentación equivalente
- Solo conceder acceso a terceros a Activos de información de ManpowerGroup según las necesidades comerciales y que requieran la aprobación por escrito de un ejecutivo autorizado de ManpowerGroup o su delegado

CICLO DE VIDA DE DESARROLLO DE SOFTWARE (SDLC en inglés)

Los esfuerzos de desarrollo de aplicaciones siguen el proceso SDLC seguro definido, donde los requisitos de seguridad son definidos, documentados y probados. El desarrollo de aplicaciones asegura que se utilicen prácticas de codificación seguras y se evidencien a través de evaluaciones de seguridad previas. Además, se publican materiales educativos para desarrolladores sobre codificación segura y se ha implementado una estricta separación de funciones entre entornos de producción y no producción.

Evaluación de riesgos

DE ADENTRO HACIA AFUERA:

Nos evaluamos continuamente y ajustamos nuestras defensas en tiempo real.

1 **Recopilación de datos e identificación de activos de información**

El primer paso en nuestro proceso de evaluación de riesgos es recopilar información de nuestros expertos comerciales y técnicos en la materia. Se recopila documentación de evidencia tanto técnica como no técnica, así como informes de indicadores clave de rendimiento (KPI).

2 **Análisis de riesgos**

El estándar de clasificación de datos de ManpowerGroup nos permite clasificar y jerarquizar rápidamente los activos de información según su función, criticidad de los datos que respaldan y la confidencialidad de los datos creados, accedidos, almacenados, transmitidos o procesados.

Los controles se evalúan periódicamente para determinar su eficacia protectora y/o detectivesca. No se supone que sean completamente efectivos, por lo tanto, la coherencia de los reportes ayuda a evaluar su impacto. Estas revisiones incluyen controles físicos y técnicos y se aplican tanto a las operaciones de ManpowerGroup como a las funciones de terceros. Los indicadores clave de rendimiento se utilizan para identificar qué controles requieren atención y se toman medidas acordes. Y luego el ciclo se repite.

Como parte del proceso de evaluación de riesgos, evaluamos continuamente las posibles amenazas y vulnerabilidades.

- Vulnerabilidades: debilidades de la solución o lagunas de control que, en caso de explotar, podrían dar lugar a divulgación autorizada, uso indebido, alteración o destrucción de los activos de información.
- Amenazas: agentes potenciales para explotar una vulnerabilidad

3 **Asignación de calificaciones de riesgo**

El último paso es asignar una calificación (Alta, Media o Baja) para cada activo de información. La calificación es la culminación del inventario de activos de información, la clasificación de activos, la evaluación de amenazas y vulnerabilidades y la evaluación de la eficacia del control.

4 **Enjuague, Repita**

El proceso de evaluación de riesgos es un ciclo constante de autoevaluación y corrección.

DE AFUERA HACIA ADENTRO: Mantenerse alineado con un panorama de amenazas cambiante

Cada año, un evaluador externo independiente realiza una evaluación de riesgos/amenazas para evaluar la eficacia de nuestro programa en el contexto de un panorama de seguridad que cambia rápidamente. Esta evaluación, junto con las métricas y los indicadores clave de rendimiento (KPI), se informa a la Alta Dirección y a la Junta Directiva. También se realizan evaluaciones independientes adicionales a lo largo del año por parte de terceros y clientes, así como auditorías internas y externas. Los resultados se comparten con el equipo de seguridad de la información y las actividades de corrección se desarrollan e integran en los proyectos en curso/actividades diarias del equipo de seguridad de la información y sus socios de apoyo.

Control de acceso

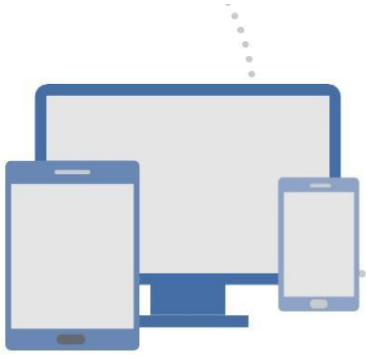
Para salvaguardar nuestros activos de información, el acceso está limitado a entidades autorizadas y justificadas por negocios con una "necesidad de saber". Hemos tomado medidas exhaustivas para evitar el uso inadecuado de las credenciales de acceso:

- Requerir una autenticación fuerte y monitorear todo acceso a información confidencial
- Emitir credenciales de autenticación únicas de acuerdo con el "privilegio mínimo" y separadas de los ID de usuario estándar a nivel de usuario.
- Deshabilitar todo el acceso al sistema después de un período de inactividad
- Supervisar toda la infraestructura de red, hardware y software mientras se usa el acceso privilegiado
- Cambiar el acceso predeterminado y las configuraciones proporcionadas por los proveedores de hardware y software
- Encriptar la información compartida en comunicaciones digitales exigida por ley, regulación o acuerdo contractual
- Requerir autenticación multifactorial (MFA) para todos los accesos remotos

Protección física y ambiental

Los procesos y procedimientos protegen contra el acceso físico no autorizado, el daño y la interferencia con las operaciones comerciales:

- Proteger áreas seguras con barreras de seguridad y controles de entrada definidos
- Protección física de todos los activos de información, como archivos en papel, dispositivos de usuarios finales, servidores, dispositivos de red, bases de datos, dispositivos de almacenamiento y copias de seguridad contra accesos no autorizados, daños e interferencias
- Instruir a los empleados para que bloqueen los sistemas desatendidos y aseguren su entorno de trabajo.
- Asegurar las instalaciones contra el acceso no autorizado según las leyes, reglamentos y requisitos contractuales aplicables.
- Garantizar que la retención y destrucción de la información siga la Políica de Retención de Registros de ManpowerGroup.



TECNOLOGÍA

Monitoreo de Actividad, Análisis y Respuesta a Eventos de Seguridad

MONITOREO DE LA ACTIVIDAD

ManpowerGroup ha establecido una solución de Monitoreo de Eventos e Información de Seguridad (SIEM, siglas en inglés) en toda la organización, que recopila información de eventos de los dispositivos de ManpowerGroup (p. ej., IDS/IPS, HID, registros de eventos del sistema y firewalls) y la envía al Centro de Operaciones de Seguridad (SOC) para su análisis detallado. El SOC correlaciona y analiza los datos para identificar posibles comportamientos/actividades maliciosas. El SOC también utiliza información de análisis de amenazas de terceros para ayudar en la identificación de indicadores de compromiso (IOC) que pueden existir dentro del entorno de ManpowerGroup.

ANALIZANDO Y RESPONDIENDO

ManpowerGroup utiliza un sistema de seguimiento de incidentes para documentar y rastrear eventos de seguridad que incluyen:

Entrada del evento

Eventos informados al equipo de seguridad o identificados por el SOC, donde un miembro designado del equipo de seguridad asume la propiedad del evento y la responsabilidad de actualizar el sistema de seguimiento y escaladas cuando sea necesario.

Seguimiento

El seguimiento se realiza en todos los eventos abiertos para documentar los detalles de la investigación, impulsar la rendición de cuentas y garantizar el cierre oportuno. Las medidas de escalada aseguran que las partes apropiadas estén informadas y que se cumplan los requisitos necesarios, especialmente en una situación en la que se requiere una escalada oportuna como parte del cumplimiento normativo y/o el cumplimiento de un acuerdo contractual establecido. Además, se determina la causa de fondo y la parte responsable para ayudar a corregir el incidente.

Corrección

La corrección puede requerir la participación de varios equipos y partes externas. El equipo de seguridad de la información brinda orientación o dirección sobre las medidas correctivas apropiadas.

Cierre del incidente

Un incidente se clasifica como cerrado después de que se ha reunido evidencia para confirmar que se han realizado las acciones correctivasy/o medidas preventivas requeridas o que el riesgo se ha mitigado a un nivel apropiado que requiere la aprobación de la alta dirección.

Lecciones aprendidas posteriores al cierre

Después del cierre formal, se lleva a cabo una revisión holística del incidente, incluido el análisis de la causa de fondo, la revisión de las comunicaciones y las oportunidades de mejora en el proceso general de respuesta/corrección.

Encriptado

Nuestros controles de encriptado garantizan que la información confidencial permanezca confidencial y protegida mientras está en reposo o en movimiento. Las protecciones incluyen:

• Implementar un estándar de encriptado que defina los requisitos para encriptar información confidencial y garantice elcumplimiento de los requisitos legales, reglamentarios y contractuales.

• Encriptar información confidencial cuando se almacena o transmite a través de redes públicas

• Encriptar conexiones de acceso remoto en nuestro ecosistema

• Requerir la aprobación del CISO para métodos de encriptado no estándar

Malware

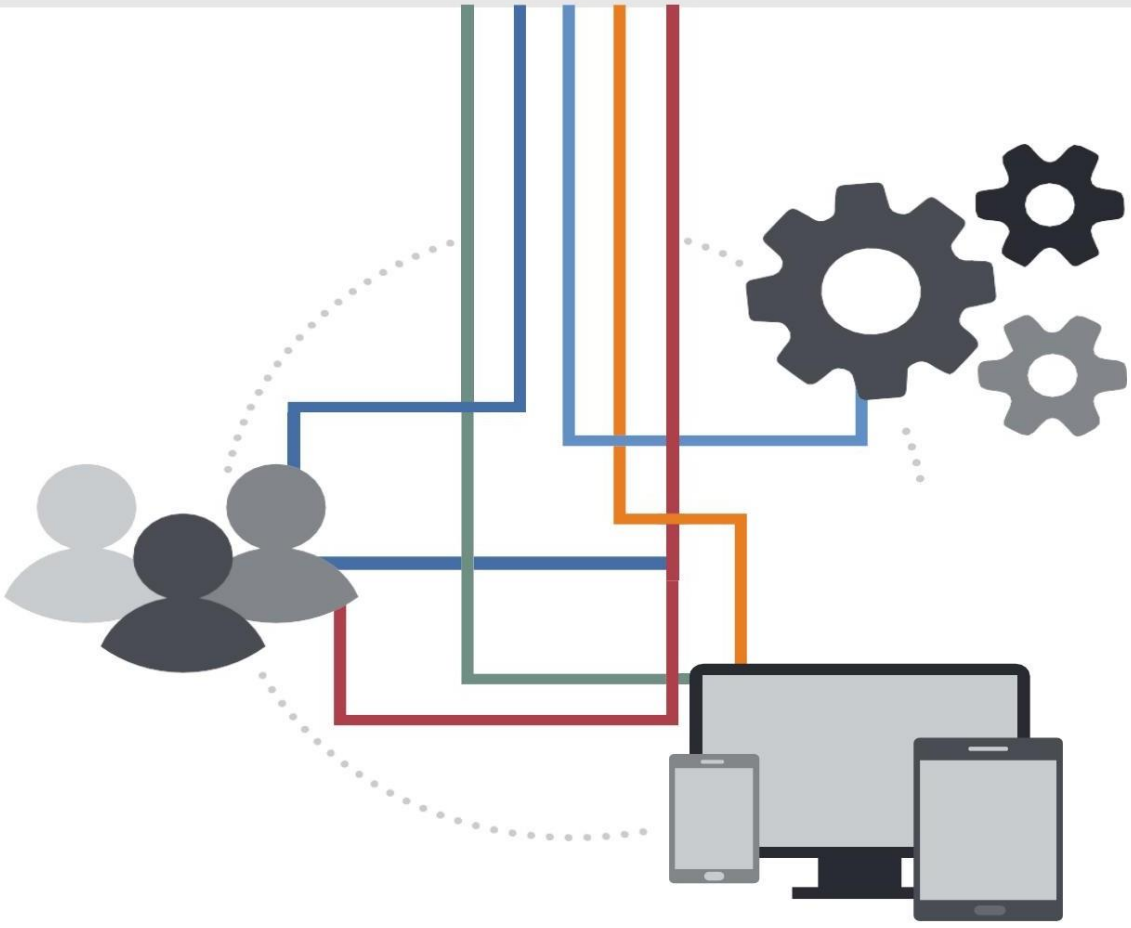
Protegemos de la ejecución de código malicioso (Malware) a través de actividades que incluyen:

- Confirmar nuestros controles de seguridad a través de auditorías periódicas
- Supervisar y registrar sistemas y eventos
- Proteger las instalaciones de registro del sistema de información y la información de registro contra manipulación y acceso no autorizado.
- Sujetando todo el hardware y software a adherirse al programa de gestión de vulnerabilidades que incluye protección antivirus, parches de seguridad y prácticas reconocidas por la industria para el fortalecimiento y defensa de los activos.
- Exigir a las estaciones de trabajo y servidores instalar, configurar y mantener software de protección de extremos.
- Escanear aplicaciones web abiertas al público en busca de vulnerabilidades, al menos anualmente.
- Implementar campañas de educación y campañas periódicas para el usuario final.
- Utilizar tecnología web y de correo electrónico para escanear o identificar malware antes de que ingrese a nuestro entorno.

Continuidad del negocio

Nuestro programa de continuidad del negocio garantiza la resiliencia de las operaciones comerciales de ManpowerGroup a través de un framework integral de respuesta y recuperación que incluye:

- Un proceso formal de análisis de impacto comercial que identifica los procesos críticos y los habilitadores de TI
- Evaluaciones de riesgos que identifican y priorizan los riesgos relacionados con la confidencialidad, integridad y disponibilidad
- Un Plan de Continuidad del Negocio (PCN) que se revisa, actualiza y distribuye periódicamente.
- Estrategias integrales de copia de seguridad y recuperación que garantizan Objetivos de Tiempo de Recuperación (RTO siglas en inglés) y Objetivos de Punto de Recuperación (RPO siglas en inglés)
- Capacitación, concientización y pruebas



Contáctenos

Agradecemos su interés en nuestra Política de Seguridad de la Información y lo alentamos a que se involucre más con la protección de sus datos. Si tiene alguna pregunta sobre cómo ManpowerGroup protege su información, así como la información que se nos confía, comuníquese conmigo directamente. Si desea saber más sobre nuestro programa, no dude en solicitar una reunión con nosotros. En nombre de ManpowerGroup y de todo el equipo de Seguridad, esperamos con ansias trabajar con usted.

Randy L. Herold

Director de Seguridad de la Información

randy.herold@manpowergroup.com

Obtenga más información sobre nuestra Política y prácticas de seguridad de la información: https://www.manpowergroup.com/sustainability/infosecprivacy

ManpowerGroup