Ciberseguridad:

Guía de implementación para empresas

Septiembre 2023

Contenidos

Introducción

La Ciberseguridad se ha convertido en una prioridad crítica en la era digital actual.

A medida que nuestra empresa depende cada vez más de la tecnología y el almacenamiento digital de información, enfrenta riesgos significativos de ciberataques y pérdida de datos.

Esta guía proporciona un plan paso a paso para implementar la ciberseguridad en su compañía, asegurando la protección de activos digitales y la continuidad del negocio.

Objetivos de la Implementación de Ciberseguridad

01

Proteger los activos digitales, incluyendo datos confidenciales, propiedad intelectual y sistemas críticos, de amenazas cibernéticas.

02

Minimizar el riesgo de brechas de seguridad que podrían dañar la reputación de la empresa y resultar en costos significativos.

03

Cumplir con regulaciones y normativas de seguridad de la información específicas de su industria.

Beneficios de la Implementación de Ciberseguridad

- Reducción del riesgo de pérdida de datos y brechas de seguridad
- Protección de la reputación de la empresa y la confianza de los clientes
- Cumplimiento normativo y evitación de sanciones financieras
- Continuidad del negocio y disponibilidad de servicios críticos

Costos de Implementación

Presupuesto inicial para la implementación de medidas de ciberseguridad.

Costos operativos continuos para mantener y mejorar las medidas de seguridad.

Retorno de la Inversión (ROI)

La inversión en ciberseguridad se espera que resulte en una reducción significativa del riesgo de incidentes de seguridad costosos.

Evitar incluso un incidente importante puede amortizar la inversión de manera significativa.

Pasos a Seguir

1

Roles Clave: CEO, CIO, CISO, CFO, COO

Paso 1: Compromiso
de la Alta Dirección

La alta dirección debe comprender la importancia de la ciberseguridad y comprometerse con su implementación. Esto incluye asignar recursos y presupuesto adecuados para las iniciativas de ciberseguridad.

2

Rol Clave: Analista de Riesgos

Paso 2: Evaluación
de Riesgos y Activos Críticos

Realice una evaluación exhaustiva de los riesgos de ciberseguridad que enfrenta la empresa. Identifique los activos críticos, como datos confidenciales, propiedad intelectual y sistemas esenciales, para priorizar las acciones.

3

Roles Clave: Ingeniero de Ciberseguridad, Analista de Ciberseguridad

Paso 3: Definición
de Políticas y Procedimientos

Desarrolle políticas y procedimientos claros de seguridad de la información que se adapten a las necesidades específicas de su empresa. Esto debe abordar temas como contraseñas, acceso a sistemas y datos, uso de dispositivos y redes y respuesta a incidentes.

Pasos a Seguir

4

Roles Clave: Recursos Humanos, Equipo de Ciberseguridad

Paso 4: Educación
y Capacitación

Implemente un programa integral de concienciación en ciberseguridad para todos los empleados. Esto incluye capacitación en reconocimiento de amenazas, uso seguro de sistemas y aplicaciones y reporte de incidentes.

5

Roles Clave: Recursos Humanos, CISO, Gerente de Contratación

Paso 5: Contratación y Formación
de un Equipo de Ciberseguridad

Identifique las habilidades y competencias necesarias para los roles de ciberseguridad y realice procesos de contratación rigurosos. Proporcione oportunidades de capacitación y desarrollo continuo para el equipo.

6

Paso 6: Implementación
de Medidas Técnicas

Introduzca medidas técnicas de seguridad, como firewalls, sistemas de detección de intrusiones, cifrado de datos y autenticación multifactorial (MFA). Asegúrese de mantener sus sistemas actualizados y protegidos.

Pasos a Seguir

7

Paso 7: Plan
de Respuesta a Incidentes

Desarrolle un plan detallado de respuesta a incidentes que incluya procedimientos para manejar posibles brechas de seguridad, para ello es recomendable tener ISMS (Information Security Management System) dicho sistema cubre temas desde la gestión de riesgos, plan de continuidad, detección, monitoreo, entre otros.

8

Paso 8: Monitoreo
y Mejora Continua

Implemente sistemas de monitoreo continuo para detectar actividades sospechosas y realice pruebas de penetración y evaluaciones de seguridad periódicas. Ajuste y mejore constantemente las medidas de ciberseguridad según los resultados.

9

Rol Clave: Analista GRC (Gobierno, Riesgo y Cumplimiento)

Paso 9: Cumplimento
Normativo

Asegúrese de cumplir con las regulaciones y leyes relacionadas con la ciberseguridad en su industria o región. Mantenga registros adecuados para demostrar su cumplimiento.

Pasos a Seguir

10

Paso 10: Cultura
de Seguridad

Fomente una cultura de seguridad en toda la empresa, donde cada empleado comprenda su papel en la ciberseguridad y sea consciente de las amenazas potenciales.

11

Paso 11: Comunicación
Interna y Externa

Comunique sus esfuerzos en ciberseguridad tanto interna como externamente. Esto puede ayudar a construir confianza y demostrar su compromiso con la seguridad.

12

Paso 12: Evaluación
y Actualización Periódica

Revise y actualice regularmente su estrategia y medidas de ciberseguridad para mantenerse al día con las amenazas emergentes y los cambios tecnológicos.

¿Cómo podemos ayudarte?

Evaluación de Riesgos

Realizamos evaluaciones exhaustivas de riesgos para identificar vulnerabilidades y amenazas cibernéticas en su infraestructura digital.

Diseño de Estrategias de Seguridad

Desarrollamos estrategias personalizadas de ciberseguridad que se alinean con los objetivos y recursos de su empresa.

Capacitación y Concienciación

Ofrecemos programas de formación en ciberseguridad para capacitar a su personal en el reconocimiento de amenazas y buenas prácticas de seguridad.

Implementación de Soluciones Técnicas

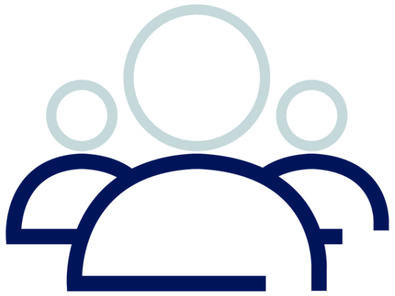
Realizamos evaluaciones exhaustivas de riesgos para identificar vulnerabilidades y amenazas cibernéticas en su infraestructura digital.

Respuesta a Incidentes

Desarrollamos planes de respuesta a incidentes para gestionar de manera efectiva posibles brechas de seguridad a través de un equipo especializado.

Cumplimiento Normativo

Le asistimos en el cumplimiento de regulaciones relacionadas con la ciberseguridad en su industria.



¿Quiénes somos?

Gi Group Holding es el mayor ecosistema global de soluciones integradas de capital humano. Contribuimos en el desarrollo del mercado laboral sostenible, entregando apoyo ante las diversas necesidades que presentan las empresas.

Contamos con una división especializada en Tecnología de la información, tenemos una solución enfocada en los profesionales tecnológicos, creativos y digitales.

Aplicamos un enfoque de consultoría en todas nuestras soluciones para comprender completamente las dinámicas de cada sector y lugar de trabajo.

¿Por qué elegirnos ante tus necesidades de Ciberseguridad?

Experiencia y Conocimientos:
Contamos con un equipo de expertos en ciberseguridad con experiencia en diversas industrias.

Enfoque Personalizado:
Adaptamos nuestras soluciones a las necesidades específicas de su empresa.

Actualización Constante:
Mantenemos nuestro conocimiento actualizado para abordar las amenazas emergentes.

Compromiso con su Éxito:
Nuestro objetivo es proteger sus activos digitales y garantizar la continuidad de su negocio.

En Gi Group Holding comprendemos los desafíos relacionados con la protección de activos digitales y la mitigación de amenazas cibernéticas son cruciales para el éxito y la continuidad de su negocio.

Juntos, podemos construir una estrategia sólida para proteger sus activos y asegurar su éxito en un entorno digital en constante evolución.

Este material ha sido desarrollado por el equipo de negocios de Gi Group Holding en Chile, junto a nuestro consultor especialista y CTO, Douglas Bellon Rocha.

¡Nos gustaría conversar contigo para encontrar la mejor solución para tu empresa!

Gi Group HOLDING

More than **Work**

Carlos Echevarria

carlos.echevarria@gigroup.com

Escanea acá

escribir a Carlos