Plan de Ciberseguridad

Un cambio en el modelo … de lo reactivo a lo proactivo

Forensic CORP
PREVENTION AND RESPONSE

Los sistemas de información y la plataforma tecnológica que los soportan, hoy en día son unos de los activos principales de las organizaciones, por lo que ha surgido la necesidad imperante de que las empresas deban implementar procedimientos y controles que ayuden a minimizar los riesgos de amenazas a los que se ven expuestas y que puedan afectar la confidencialidad, integridad o disponibilidad de dicha información, ante lo cual es recomendable implementar controles mínimamente necesarios a través de la aplicación de un plan de buenas prácticas y plataformas tecnológicas que permita minimizar sus probabilidades de ocurrencia.

Objetivos del Servicio

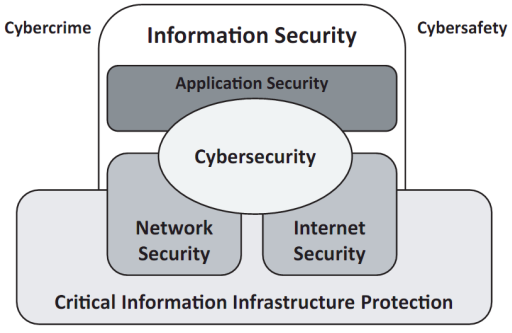
- **Implementar** un marco de trabajo e infraestructura tecnológica que permita la preparación, protección, detección, investigación y monitoreo ante los eventos de seguridad.
- **Disminuir** la ocurrencia y efectividad de ataques de hacking, software malicioso (Malware) u otros programas no deseados, que atenten contra la integridad, disponibilidad o confidencialidad de la información perteneciente a la organización.
- **Mantener** controlados los riesgos con el fin de detectar oportunidades de mejora y disminuir la probabilidad de ocurrencia de hechos delictuales.
- **Asegurar** la privacidad y confidencialidad tanto de la organización, así como también de las entidades externas (consumidores y/o proveedores) con las que interactúa y que participan en procesos de intercambio de información.
- **Disminuir** la probabilidad de que la organización sea víctima de fraudes corporativos, a través del control de los sistemas tecnológicos que soportan y administran el acceso a las plataformas de gestión empresarial.

Alcance

El presente plan de acción, puede ser implementado en cualquier organización, debido a que dependiendo de los objetivos estratégicos planteados por la alta dirección, se realiza un análisis de riesgos de los activos críticos o a la totalidad de ellos, derivando en la implementación de un Plan de Seguridad que conlleva la implementación técnica y operacional de procedimientos.

Gestión e Implementación

El plan de ciberseguridad o seguridad informática, tiene por objetivo implementar procesos, políticas, procedimientos y controles (operacionales y técnicos) cuyo fin es mitigar los riesgos que afectan a los **activos de información críticos** de la organización, bajo una arquitectura de Ciberseguridad, con énfasis en el intercambio de información con terceros a través de Internet y de dominios de seguridad principales.



Por lo tanto, el servicio que colocamos a disposición de nuestros clientes para la gestión de la seguridad informática de su organización, consta de tres procesos fundamentales, que se interrelacionan para mantener un marco de trabajo que permita monitorear y gestionar los riesgos asociados a amenazas provenientes desde y hacia el ciberespacio.

PROCESOS CLAVES CYBERSEGURIDAD	Descripción
Anticipar es observar lo desconocido, sobre la base de la identificación y análisis de amenazas cibernéticas, riesgos potenciales y la toma de medidas antes de que se produzca algún daño.	Anticipar
Adaptar es ajustarse al cambio, ajustando y diseñando los sistemas de seguridad ante los cambios del entorno globalizado, focalizándose en proteger los activos de la organización ante posibles amenazas futuras.	Adaptar
Activar las medidas de seguridad, colocando en funcionamiento el conjunto de medidas de seguridad informática diseñadas para proteger la integridad del negocio y su patrimonio.	Activar

Cybersecurity
FORENSIC SECURITY FOR ENTERPRISE

Plan de Ciberseguridad

El servicio de Ciberseguridad consta de actividades específicas para gestionar la seguridad, que pueden ser contratadas de acuerdo a las necesidades de la organización, las cuales se realizan con la periodicidad definida por nuestros clientes.

Servicios de Implementación Tecnológica

N°	Servicio	Periodicidad	Descripción
I1	Diseño e implementación arquitectura de ciberseguridad	Inicial	Implementación de equipos informáticos de seguridad, que permitan aislar la red interna de la red pública, así como también permita gestionar los accesos físicos y lógicos de los usuarios que la utilizan, con el fin de resguardar los activos de información que se interconectan a esta.
I2	Implementación de procedimientos de seguridad de procesos críticos.	Inicial	Implementación de procedimientos y controles de seguridad, relacionados con los procesos críticos que influyen en el resguardo de la seguridad de los activos de información, tales como permisos de acceso de a la red de datos, políticas de gestión de usuarios y empleados, gestión de permisos a proveedores, entre otros.)

Servicios Mantenimiento

N°	Servicio	Periodicidad	Descripción
M1	Escaneo y limpieza de malware	Mensual Trimestral	Ejecución de procedimientos preventivos y reactivos de escaneo y limpieza de Malware (Virus, gusanos, troyanos, etc.) que podría estar presente en los equipos computacionales de usuarios, a través del uso de antivirus actualizados y/o software especializado
M2	Actualización y mantención de Antivirus	Mensual Trimestral	Administración y mantención de software antivirus, con el fin de prevenir la presencia de Malware (Virus, gusanos, troyanos, etc.) que pueda afectar los equipos computacionales de los usuarios.
M3	Desfragmentación discos duros	Mensual Trimestral	Ejecución de procedimientos preventivos de desfragmentación de los dispositivos de almacenamiento (discos duros) presentes en los equipos computacionales, con el fin de optimizar su rendimiento y/o detectar problemas de operación de estos.
M4	Revisión y actualización de parches de seguridad	Mensual Trimestral	Revisión periódica e instalación de parches de seguridad de los Sistemas Operativos y Software principal, que se encuentran presentes en los equipos computacionales de los usuarios.
M5	Formateo y reinstalación de computadores	Mensual Trimestral	Formateo de dispositivos de almacenamiento (discos duros), instalación y configuración del Sistema Operativo, instalación de software básico para su operación o utilización por parte de los usuarios.
M6	Instalación y configuración de servicios de impresión	Mensual Trimestral	Instalación y configuración de impresoras o servicios de impresión, así como también la instalación y configuración del software y/o drivers necesarios para su utilización por parte de equipos computacionales de usuarios.
M7	Mantención física de equipos computacionales	Mensual Trimestral	Mantención física de equipos computacionales, el cual consiste en una limpieza exterior e interior de dicho equipamiento, con el fin de evitar daños al hardware electrónico por condensación u otros problemas similares.

Servicios Gestión de Seguridad

N°	Servicio	Periodicidad	Descripción
O1	Monitoreo y análisis de eventos de seguridad	Diario Semanal	Revisión y análisis de eventos de seguridad detectados y registrados por los servicios de red y seguridad implementados, con el fin de detectar y reaccionar ante incidentes de seguridad que puedan afectar a la organización, así como también diseñar e implementar las mejoras necesarias para evitar su recurrencia en el futuro.
O2	Administración de servicios de seguridad lógica de acceso a la red de datos (cableada y/o inalámbrica)	Ante Requerimiento	Administración de accesos a la red interna de la organización (cableada e inalámbrica) a través de la ejecución de procedimientos específicos que resguarden y controlen la seguridad de los activos de información conectados a estas (equipos computacionales, sistemas y otros recursos de red), lo cual conlleva la administración de firewalls, routers, puntos de acceso, entro otros., lo cual permite minimizar los riesgos de que las amenazas se materialicen disminuyendo su probabilidad de ocurrencia.
O3	Administración de usuarios y equipos computacionales	Ante Requerimiento	Administración de permisos de accesos de los usuarios que componen la organización, de acuerdo a las políticas y perfiles definidos a sus funciones, a través de la administración de Active Directory y otros servicios complementarios.
O4	Análisis forense de incidentes de seguridad	Ante Evento	Análisis forense de evidencias digitales, cuando incidentes de seguridad afectan activos de información de relevancia, con el fin de determinar el modus operandi y responsables en el incidente, con el fin de prevenir su recurrencia en el futuro, así como también poseer los medios de prueba necesarios para establecer las acciones legales o contractuales correspondientes a su relevancia.