Seguridad de la Información y Confidencialidad

Departamento IT

Ership
Grupo

Conceptos Previos

Definiciones generales de Seguridad Informática

Seguridad Informática

Se refiere a los sistemas que permiten proteger las infraestructuras tecnológicas implantadas en la organización (almacenamiento, servidores, comunicaciones, etc ..)

Seguridad de la Información

Se refiere a la protección de los activos de información necesarios para la organización.

Activo de Información

Es todo aquello que en la organización se considera importante y que puede contener información como puede ser archivos, bases de datos, cuentas de usuario, contraseñas, correo electrónico, etc …

Fuentes de Información

Son los orígenes que crean el activo de información como puede ser OpycNet, Iris, un archivo adjuntado en un correo electrónico, Inca, archivos creados por los usuarios, etc …

SGSI

Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI) es, básicamente un conjunto de políticas de administración de la información en búsqueda de proteger sus activos de información esenciales para la continuidad del negocio.

El objetivo de un SGSI es implementar y monitorizar la seguridad informática de la organización para que esta pueda lograr sus objetivos comerciales y/o de servicio.

Planificar

Se evalúan los riesgos de seguridad de la información y se seleccionan los controles adecuados

Verificar

Revisar y evaluar el correcto funcionamiento de los controles definidos

Hacer

Fase de implantación del los controles definidos

Actuar

Fase en la que se realizan cambios para mantener los controles definidos

Política Continuidad del Negocio

Un error común es pensar que el SGSI es una cuestión meramente tecnológica y que únicamente afecta al departamento de IT.

El SGSI es una directiva de alta dirección para garantizar el ciclo de vida de la organización y que tenemos que respetar e impulsar todas las personas que trabajamos en la organización.

Toda la organización debe de implicarse en tomar las medidas necesarias para garantizar la seguridad de la información y la seguridad informática.

La información es poder y hay que tener procedimientos definidos para garantizar su acceso y disponibilidad. Esta información normalmente se define como valiosa, crítica o Sensible.

Toda información tiene carácter confidencial con lo que hay que establecer mecanismos de acceso a usuarios para evitar un acceso indebido.

La función del departamento de IT es hacer realidad todas las medidas necesarias para asegurar la continuidad del negocio y marca unas normas de comportamiento que tiene que ser asumidas y apoyadas por todos los integrantes de la organización.

Protocolo Seguridad de la Información

Estrategia de empresa a largo plazo para evitar riesgos derivados de la falta de seguridad en la información en la ejecución de las decisiones de negocio.

Este Protocolo de Seguridad de la Información, adjunto a esta formación, forma parte del Sistema de Cumplimiento Normativo del Grupo y es de aplicación en todas las sociedades que integran el Grupo Ership.

Las normas son de obligado cumplimientos por todos los trabajadores del Grupo Ership con independencia de su nivel jerárquico

- No se destruirá, alterará o inutilizará de ninguna forma la información relevante.
- No se enviarán mensajes calificados como SPAM desde medios proporcionados por el grupo Ership.
- No se instalarán ni descargarán programas informáticos sin previo conocimiento del departamento IT.
- No se enviará información sensible a ningún tercero sin conocimiento previo del responsable.
- No se utilizará el email del grupo Ership para el envío o recepción de datos ajenos a las labores del puesto de trabajo.
- No se abrirán documentos adjuntos o enlaces en correos electrónicos sin comprobar el remitente. Ante cualquier duda en un email sospechoso contactar con el área de Sistemas del departamento IT.
- Se tendrá especial cuidado con correos electrónicos en los que nos informen de un cambio en las condiciones comerciales (cambios cuenta corriente) de nuestros proveedores/clientes. Ante cualquier cambio, contactar telefónicamente con el tercero para confirmar la información.
- Las credenciales de acceso a los sistemas informáticos son únicas e intransferibles.
- No conceder el control remoto del equipo a ningún tercero sin aprobación previa del departamento de IT.

Protección de la Información

Con objeto de asegurar la protección de la información del Grupo, durante el proceso de contratación todos los trabajadores suscriben un compromiso de confidencialidad que contempla los siguientes puntos:

- Todo el personal del Grupo tiene obligación de confidencialidad y deber de secreto. Bajo ningún concepto puede revelarse a persona ajena a la organización información o documentación a la que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización escrita.

- Únicamente está permitido utilizar la información referida en el apartado anterior en la forma exigida por el desempeño de sus funciones en la empresa, sin estar permitido disponer de ella de ninguna otra forma o para otra finalidad diferente.

- Queda prohibido utilizar los recursos del Grupo a los que tenga acceso para cualquier otra finalidad diferente de las estrictamente laborales. La Dirección del Grupo se reserva el derecho a revisar el correo electrónico del personal, las sesiones de acceso a Internet, o el uso de cualquier recurso propiedad del Grupo, cuando se tengan dudas razonadas acerca de su uso inapropiado.

- Se debe trabajar siempre en el sistema de información autorizado, con los recursos y permisos concedidos para que toda actividad quede registrada. Cualquier archivo creado fuera del sistema de información establecido, por ejemplo, en el escritorio de su ordenador o mediante ficheros temporales, deberá ser eliminado cuando concluya la finalidad para la que fue creado.

- No se atenderán solicitudes de información por teléfono (excepto los casos autorizados con preguntas de seguridad) y sin la debida identificación. Como norma general, sólo están autorizadas las solicitudes de información por escrito.

- La salida de soportes informáticos, ordenadores portátiles o cualquier documentación física fuera de la organización, solo se realizará cuando sea estrictamente necesario, guardando en todo momento la debida diligencia respecto a la protección de los activos e información propiedad del Grupo.

- Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral/mercantil con Grupo Ership.

Protocolo Seguridad Informática

Estrategia de empresa a largo plazo para evitar riesgos derivados de la falta de seguridad en los sistemas informáticos/infraestructura en la ejecución de las decisiones de negocio.

- El Grupo Ership dispone de sistemas de seguridad perimetral (Firewall) que permite el control del tráfico hacia y desde Internet.
- El Grupo Ership dispone de un servicio Anti Spam para que el correo electrónico sea filtrado de Spam y otros ataques informáticos.
- El Grupo Ership dispone de un servicio de anti virus para la detección y eliminación de virus informáticos.
- El Grupo Ership dispone de una plataforma de ciber seguridad (DarkTrace) que monitoriza constantemente todo el tráfico de datos y detecta comportamientos sospechosos pudiendo tomar decisiones autónomas o bajo demanda que permiten cortar el tráfico y evitar problemas derivados.
- El Grupo Ership dispone de un departamento interno (IT Sistemas) que es el encargado de gestionar la seguridad informática. Es muy importante que ante cualquier duda de correo sospechoso, archivo extraño, etc .. Contactar con ellos para su supervisión.
- El Grupo Ership dispone de unas políticas de Backup de la información que garantizan la recuperación de la misma en situaciones concretas. Es muy importante que los usuarios almacenen la información importante en los recursos de red (Unidades U, G, …) que es el origen de los backups de la información. Estos Backups se realizan sobre datos (archivos, correos, etc ..) y también de sistemas.

El Usuario … el eslabón más débil de la cadena !!

En lo referente a la seguridad informática el usuario es el eslabón más débil. Para evitar (o minimizar) el riesgo de ataques informáticos, el usuario debe:

- No descargar archivos de internet, ni visitar páginas web “desconocidas”.
- No conectar dispositivos ajenos a los equipos informáticos del Grupo.
- No instalar por propia iniciativa ningún producto informático en ordenadores y sistemas de información de la organización.
- Plantearse las siguientes preguntas ante cualquier correo electrónico recibido:

  - ¿Conozco al remitente?
  - ¿Esperaba el correo electrónico?
  - ¿Reconozco el archivo adjunto?

  Siempre aplicar sentido común y si recibimos algún correo extraño de un proveedor/cliente, antes de nada, hablar con IT o bien con el tercero.

Y lo más importante, ante cualquier duda, consultar con el departamento de IT, estamos para ayudaros !

ERSHIP Grupo
Lagasca, 88
28001 Madrid (España)

+34 914 263 400
www.ership.com