Políticas de Seguridad de la Información

Resumen

Objetivo de aprendizaje:

Aprender a aplicar las medidas de protección necesarias para que la seguridad de la información se mantenga en el entorno laboral rigiéndose por la Política de Seguridad de la Información de la Empresa.

Seguridad de la Información

La Política General de Seguridad de la Información de la empresa tiene por objetivo dar continuidad a los procesos operativos, protegiendo los activos de información frente a amenazas internas y externas que atentan contra la confidencialidad, la disponibilidad e integridad de datos.

Riesgos a los que nos enfrentamos:

- *Pérdida de Clientes.*
- *Daño a la imagen y reputación.*
- *Inclumplimiento legal y regulartorio.*
  Ejemplo: Ley de protección de datos.
- *Paralizacion de las operaciones en procesos críticos por falla en sistemas.*
- *Pérdida financiera.*

Por lo tanto, hay que tomar las acciones necesarias para proteger la información y los sistemas claves para el funcionamiento del negocio con el fin de mitigar las amenazas y riesgos que puedan poner en peligro la competitividad, rentabilidad y legalidad necesaria para alcanzar los objetivos de negocio.

Malware

Una de las amenazas más comunes y a la que estamos expuestos es a la infección por algún Malware. Al estar infectados los atacantes pueden robar información, espiar las actividades realizadas en el computador, hacer chantajes, secuestrar datos e infectar toda la red laboral.

Las medidas de protección que debemos aplicar para combatir las amenazas por malware son:

- *Mantener software de antivirus instalado y actualizado.*
- *Al visitar sitios Web verificar que sea un sitio seguro (HTTPS).*
- *Nunca abrir links enviados por correo electrónico de origen desconocido o no confiable.*
- *Nunca abrir archivos adjuntos en correos electrónicos de fuentes desconocidas.*
- *Si viajas con un computador, siempre llevarlo como equipaje de mano, y no dejarlo a la vista en automóviles o lugares públicos.*
- *Mantener las fuentes de información confidencial con control de acceso y fuera del alcance de quienes no deban acceder.*
- *Bloquear el computador cuando quede desatendido, (bloqueo rápido: Windows + L).*
- *No guardar contraseñas escritas en lugares visibles o de fácil acceso como agendas, bajo el teclado, etc.*
- *No utilizar pendrive o dispositivos de almacenamiento que puedan contener algún Malware.*

Ingeniería Social

Otra de las amenazas que podemos enfrentar es a través de técnicas de Ingeniería Social.

Las amenazas realizadas por ingeniería social se pueden llevar a cabo a través de un sitio conocido por la víctima, solicitado información a través de correo electrónico, mensaje de texto e inclusive por medio de una llamada telefónica de falsos centros de atención.

Las recomendaciones a seguir para evitar los ataques por ciberdelincuentes son:

1. No abrir links ni archivos adjuntos de correos electrónicos de fuentes desconocidas, siempre verificar el origen.
2. No entregar datos sensibles a desconocidos mediante llamadas telefónicas, correos electrónicos o cualquier medio de comunicación.
3. Nunca dar acceso a las instalaciones de la empresa a terceros sin previa autorización.

Control de Acceso

Los controles de acceso permiten que los usuarios accedan sólo a los recursos para los que están autorizados e impide que usuarios no autorizados puedan acceder a información confidencial.

Se deben mantener mecanismos de control de acceso sobre lo físico (seguridad física) y sobre la información (seguridad lógica) con el fin de proteger la empresa completamente.

Medidas de protección

Medidas de protección para el control de acceso físico:

- *No dejar ingresar a las instalaciones a personas desconocidas que no porten credencial de visita.*
- *Si ves a una persona sospechosa habla con ella y pregúntale qué necesita derivándolo a la recepción.*
- *Respetar los controles y condiciones de acceso físico a las instalaciones.*
- *Informar cualquier falla o violación de los controles de acceso físico a las instalaciones por personal no autorizadas.*

Medidas de protección para el control de acceso lógico:

- *No utilizar contraseña de los compañeros de trabajo para ingresar a sistemas a los cuales no se tiene acceso.*
- *Mantén protegidas tus contraseñas de acceso a los sistemas.*
- *Solicitar a la mesa de ayuda desbloqueo o reasignación de contraseñas.*
- *Si te das cuenta de alguna falla en los controles de acceso lógicos de los sistemas debes informarlos.*

Escritorio y pantalla despejada

Mantener el escritorio y pantalla despejada es clave para evitar el extravío o hurto de información importante para el negocio, siempre está el riesgo de que alguien ajeno a la empresa ingrese a las instalaciones con el fin de obtener información valiosa con la cual se pueda lucrar.

Medidas de protección:

Los trabajadores de la empresa deben mantener el puesto de trabajo libre de documentos considerados críticos, idealmente despejado y limpio.

La documentación debe ser guardada y clasificada según su importancia.

La información restringida o confidencial debe almacenarse bajo llave o aplicar cualquier tipo de bloqueo de acceso físico que asegure que no se verá afectada su confidencialidad.

Los colaboradores no deben dejar notas o papeles con las claves de acceso expuestas o visibles por terceras personas.

Toda vez que el usuario no use su computador debe apagarlo o habilitar el protector de Pantalla con contraseña u otro mecanismo de autenticación de usuario.

La información sensible o crítica para el negocio, dispuesta en medios de almacenamiento electrónico o papel, se debe mantener guardada bajo llave cuando no se necesite, especialmente cuando la oficina esté desocupada.

Todo documento que contiene información sensible o clasificada se debe extraer inmediatamente de las impresoras.

Uso aceptable de activos

Es importante que cada colaborador maneje los activos aplicando las medidas de protección del uso aceptable de activos, ellas son:

1	*Respetar y seguir las normas establecidas.*
2	*Respetar las condiciones de uso y protección de activos de información.*
3	*No instalar, cambiar o eliminar componentes de la plataforma tecnológica sin autorización.*
4	*Solicitar la configuración y entrega de estaciones de trabajo y portátiles.*
5	*Devolver los equipos de trabajo según la pauta definida.*
6	*Evitar utilizar los recursos tecnológicos de la empresa para fines personales o ajenos a las labores de la empresa.*
7	*Proteger la imagen y propiedad de la empresa, al usar los recursos de forma ética, cumpliendo las leyes y reglamentos vigentes.*
8	*Utilizar sólo el software propietario de la empresa o aquel software que esté autorizado.*

Eliminación segura de Información

Toda información tiene una vida útil tanto si está en formato digital como si está en formatos tradicionales. Es importante emplear mecanismos de destrucción y borrado para evitar que queden al alcance de terceros y estar bajo amenazas por Trashing.

Medidas de protección:

1. *Toda información debe estar clasificada según su nivel de confidencialidad.*

2. *Cada área del negocio es responsable de la clasificación de la información que maneja.*

3. *Cada área del negocio es custodio responsable del resguardo de la información que maneja.*

4. *Si existiera la necesidad de no disponer más de alguna información es necesario destruirla utilizando los mecanismos de destrucción y borrado adecuados.*

5. *Si la información que se desea destruir está en formatos tradicionales se deberá hacer uso de una destructora de papel.*

6. *Si la información a destruir está en formato digital se deberán destruir de forma manual.*

7. *Si la información a destruir esta almacenada en un dispositivo que es reusable se deberán utilizar técnicas de borrado adecuado, por ejemplo: formatear un dispositivo de almacenamiento sobrescribiendo la información con datos vacíos, de esta manera la información anterior no es reconocible.*

Seguridad en el transporte y envío de información

La seguridad de la información también debe existir durante el envío o traslado de información, se deben aplicar controles de intercambio de información para garantizar que la misma esté protegida.

Medidas de protección:

1. *Cuando se requiera transportar información esta debe ser enviada por los medios oficiales de comunicación de la empresa.*
2. *Al transportar información física nunca debe ser desatendida y descuidada en lugares de riesgo donde pueda ser hurtada o extraviada esto incluye los equipos móviles y notebooks.*
3. *Evitar transferir información digital o física a terceros a menos que esté expresamente autorizado por los propietarios.*
4. *Seguir los procedimientos de transferencia de información.*

La seguridad de la información es responsabilidad de todos